

Appointment of a Terminal Agency Coordinator (TAC)

The FBI/NCIC requires that each department or agency possessing a computer terminal that accesses the NCIC files appoint an individual to serve as liaison and TAC for all related FBI/NCIC matters.

The selection of an individual to function as your department's TAC is entirely your decision. This individual, however, should be a supervising for management level person with a degree of authority which will ensure all FBI/NCIC policies, procedures, rules and regulations are adhered. Each agency is asked to appoint an Alternate TAC to serve with TAC is unavailable. Both the TAC and ATAC are to be NCIC certified based on the level of functionality that is assigned to the terminal located in the agency.

Some duties of the TAC include but are not limited to:

1. Receipt of all FBI/NCIC, SLED CJIS information concerning the communications network, state and national files. Ensure distribution of material within department to appropriate personnel.
 2. Receipt of monthly record validations. This includes coordinating the validation process within the department, returning the validation certification as required and investigating and assisting in resolving any problems identified with the process.
 3. Attend scheduled TAC meetings and seminars.
 4. Coordinate the scheduling of individuals for certification.
 5. Ensure compliance with all FBI/NCIC policies, procedures, etc.
 6. Responsible for the security of all terminal equipment accessing the FBI/NCIC system.
 7. Operator manual management – Secure manual, receive and update accordingly.
 8. Coordinate any relocations, etc. of the computer terminal equipment with SLED.
 9. Function as liaison as deemed necessary and appropriate during mandated audit of department's use of the FBI/NCIC system.
 10. Maintain all training records for terminal operators.
 11. Be responsible for implementing the designated reaffirmation procedure for each certified terminal operator as directed by SLED/CJIS NCIC Training.
 12. FBI CJIS Security Policy: The required **deleting of passwords, log-ons**, etc. of separated employees (4.1). For agencies using Datamaxx, Lems.Web or SNET, after SLED is notified of the separated employees, SLED will "disable" the passwords or log-ons. As per SLED ISO Sharon Baron (8-8-05), SLED Policy states that agencies should let SLED know of separated employees within 5 days upon learning of the separation. Any other vendors (DCS, etc.) will have to disable the passwords, log-ons, etc. themselves. As per SLED Policy, these agencies have 5 days to disable passwords and log-ons upon learning of the separation. This procedure must be addressed in the users written security policy.
3. The FBI CJIS Security Policy is now available to the agency TACs on Lems.Web, located at the bottom of the "Category List."

South Carolina Law Enforcement Division Criminal Justice Information System

(CJIS)

USER AGREEMENT AND SYSTEM RESPONSIBILITIES

Introduction

The South Carolina Criminal Justice Information and Communications System (CJIS) operates under a shared management concept between the South Carolina Law Enforcement Division (SLED), as the service provider, and criminal justice agencies or non-governmental agencies contracting to support certain functions for criminal justice agencies, as the service users, herein after known as "user agencies".

Criminal Justice Information and Communications System (CJIS) User Agreement

The responsibility of the SLED CJIS Division is to provide up-to-date, reliable and quality identification and information services to user agencies.

The out-of-state data (originating outside of South Carolina) provided by the SLED CJIS Division are managed and exchanged in cooperation with the FBI CJIS Division, each state CJIS Systems Agency (CSA) and Federal Service Coordinator (FSC). This information includes, but is not limited to, the Interstate Identification Index (III), the National Crime Information Center (NCIC), National Incident-Based Reporting System (NIBRS), and the Integrated Automated Fingerprint Identification System (IAFIS) programs. In addition, information is routed from all the states, Canada, and certain federal agencies via the National Law Enforcement Telecommunications System (NLETS)

The in-state data (originating within South Carolina) provided by the SLED CJIS Division are routed from and exchanged with source agencies in South Carolina. This information includes, but is not limited to, the South Carolina Central Repository for Computerized Criminal History (CCH) Record Information, the South Carolina Hot File(s), the South Carolina Incident-Based Reporting System (SCIBRS), the South Carolina Sex Offender Registry (SOR), the South Carolina Automated Fingerprint Identification System (SC AFIS), and the South Carolina GangNET® programs. Motor vehicle and motor vehicle operator data managed by the SC Department of Public Safety are routed via interface with that agency.

In order to fulfill this responsibility, the SLED CJIS Division provides the following services to its users:

- State CJIS Systems Agency and interface services for NCIC;
- State CJIS Systems Agency and interface services for NLETS;
- National Weather Service and sex offender registry;
- Operational, technical, and investigative assistance;

- Policy review of matters pertaining to III, NCIC, NIBRS, IAFIS and CCH, SCIBRS, SC SOR, SC AFIS;
- Training assistance to each terminal agency coordinator;
- Ongoing assistance to System users; and
- System and data integrity auditing.

The following documents are incorporated by reference and made part of this agreement:

- ◆ *Interstate Identification Index Operational and Technical Manual, NCIC 2000 Operating Manua and related updates (TOUS); and National Incident-Based Reporting System Volumes 1-4;*
- ◆ Minutes of the FBI CJIS Advisory Policy Board meetings;
- ◆ *Bylaws for the CJIS Advisory Policy Board and Working Groups;*
- ◆ *Title 28, United States Code, Section 534;*
- ◆ *Title 28, Code of Federal Regulations, Sections 16.30 – 16.34, Part 20, Part 25;*
- ◆ *Title 42, United States Code, Section 14611;*
- ◆ [FBI] CJIS Security Policy to include all elements of the NCIC Computerized Criminal History Program Background, Concept and Policy;
- ◆ *A Policy and Reference Manual;*
- ◆ Recommended Voluntary Standards for Improving the Quality of Criminal History Record Information, and NCIC Standards, as recommended by the [FBI] CJIS Advisory Policy Board;
- ◆ Other relevant documents to include NCIC Technical and Operational Update, CJIS Information Letter, etc.;
- ◆ *SLED Personnel Security Policy 7.6, SLED Technical Security Policies 7.6 et seq., Section 23-3-40 of the SC Code of Laws, Section 23-3-110 et seq. of the SC Code of Laws, Section 23-4-430 et seq. of the SC Code of Laws, SC Appropriations Act Proviso 56DD.8. et seq., Chapter 73 of the SC Regulations, SLED CJIS Operations Manual;*
- ◆ South Carolina Incident-Based Reporting System (SCIBRS) Guide/Training Manual;
- ◆ SLED CJIS NCIC Entry Quality Check Form (CJ-016);
- ◆ SLED CJIS Missing Person Validation Form (CJ-017); Amber Alert Information; and
- ◆ Other applicable federal and state laws, regulations, guides and forms.

The following NCIC or state files are available when direct access is authorized:

Identity Theft
Unidentified Person
Stolen Vehicle
Stolen Article
Stolen or Recovered Gun
Stolen License Plate
Wanted Person
Stolen Securities
Stolen Boat
Missing Person
US Secret Service Protective
Dept. Motor Vehicles

Foreign Fugitive
Violent Gang / Terrorist Org.
Deported Felon
Protective Order File
Interstate Identification Index
SC Sex Offender Registry
SC Criminal Histories
SC Concealed Weapons
SC Alcohol Local Option

The following limitations or conditions, if any, for specified state and/or NLETS files are made:

By accepting access as set forth above, the user agency agrees to adhere to the following NCIC and SLED CJIS policies in order to ensure continuation of that access:

1. **TIMELINESS:** (Availability, including priority of service): Agency records must be entered, modified, cleared, and canceled promptly in NCIC to ensure maximum system effectiveness. Agencies that provide NCIC access to other agencies, such as through an interface or other process for non-terminal agencies, must ensure priority service for those agencies.

Fingerprints of custodial arrest subjects taken by a law enforcement agency or detention facility for state offenses must be submitted to SLED within three workdays, and wanted persons records meeting entry criteria must be entered into NCIC immediately upon receipt of the arrest warrants by the law enforcement agency (i.e., not more than three days after).

2. **QUALITY ASSURANCE:** Appropriate and reasonable quality assurance procedures must be in place to ensure that the most complete, accurate, and valid entries are in NCIC. Pursuant to § 23-3-120 of the SC Code of Laws, a person subjected to a custodial arrest for a state offense must be fingerprinted for identification and to establish records.

3. **VALIDATION:** NCIC requires that all records except Article File records be validated 60-90 days after entry and annually thereafter. The NCIC Validation Policy is defined as:

Validation obliges the ORI to confirm the record is complete, accurate, and still outstanding or active. Validation is accomplished by reviewing the original entry and current supporting documents. Recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate source or individual also is required with respect to the Wanted Person, Missing Person, and Vehicle Files. In the event the ORI is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority must make a determination based on the best information and knowledge available whether or not to retain the original entry in the file. Validation procedures must be formalized, and copies of these procedures must be on file for review during an NCIC audit.

SLED CJIS requirements include, but are not necessarily limited to, conducting quarterly Missing Person Validations, completing the Missing Person Validation Form and the NCIC Entry Quality Check Form.

4. **HIT CONFIRMATION:** Each agency entering records must, within ten minutes or one-hour depending on priority, furnish to an agency requesting a record confirmation a response indicating a positive or negative confirmation or notice of the specific amount of time necessary to provide a response to the request for record confirmation.
5. **SECURITY:** See Technical Security Policies 7.6 (Available through SLED ISO).
6. **DISSEMINATION:** See Dissemination Policy 7.13 (Located in FBI/CJIS Security Policy & S.C Code of Laws).
7. **AUDIT:** See FBI/CJIS Security Policy. (Located on LEMS.WEB & LEO
8. **NCIC & SCIBRS TRAINING:** Each agency will be responsible for complying with mandated training requirements.

9. **PERSONNEL BACKGROUND SCREENING:** According to the FBI CJIS Security Policy, all personnel who have authorized access to FBI CJIS systems must be fingerprinted within 30 days of initial employment or assignment to include personnel directly responsible to configure and maintain computer systems and networks with direct access to FBI CJIS systems (4.5.1, (a)). Agencies should send to SLED Records on (1) completed blue applicant fingerprint card with "Criminal Justice Applicant" as the reason.
10. **LOGGING:** See Technical Security Policies.
11. **USE OF THE SYSTEM:** According to any NCIC/state policies not specifically listed above:
- A. The user agency will provide fingerprints for all custodial arrests made or brought by that agency, or ensure that they are provided, in turn, by another agency on behalf of the arresting or charging agency either via electronic submission or fingerprint card that meet submission criteria.
 - B. Each user agency with an interface to SLED CJIS must establish and maintain an information security structure that is satisfactory to the SLED Information Security Officer (ISO).
 - C. The user agency is responsible for the system access by that agency and any other agency that is, in turn, served by their agency.
 - D. Each user agency is to have a Terminal Agency Coordinator (TAC) to ensure adherence to NCIC and SLED CJIS procedures and policies within each user agency.

Acknowledgment and Certification

We hereby acknowledge the duties and responsibilities as set out in this agreement. We acknowledge that these duties and responsibilities have been developed and approved by NCIC System users in order to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in or obtained by means of the FBI / SLED CJIS Systems. We further acknowledge that a failure to comply with these duties and responsibilities will subject our access to various sanctions as approved by the [FBI] Criminal Justice Information Services Advisory Policy Board. These sanctions may include the termination of NCIC services to the agency. We may appeal these sanctions through our CJIS Systems Agency.

Name of User Agency

Address for User Agency

ORI for User Agency

Signature of User Agency Head

Title/Date

SLED:

Robert M. Stewart, Chief

BY:

Signature of CSO

Title/Date

Agencies Serviced By User Agency

Agency Name

ORI Number

Agency Name

ORI Number

Agency Name

ORI Number

Agency Name

ORI Number

Non-terminal User Agreement(s) with the above agencies must be on file with the user agency.

Revised 06/26/06

SERVICED AGENCY ADDENDUM

Authorization is hereby given to _____
Serving Agency Name

To use _____ which is issued to _____
ORI of Agency Served Name of Agency Served
and hereinafter called USER.

This authorization is for the purpose of entering, clearing, canceling, modifying or performing other authorized functions on records in the SLED CJIS (SCIC), NCIC Systems and to utilize the NLETS System and for making inquiries and messages through the _____
at _____ Serving Agency Name
ORI of Serving Agency

USER agrees to abide by all present rules, policies and procedures of SLED CJIS (SCIC), NCIC and NLETS as approved and adopted by SLED CJIS(SCIC), the NCIC Advisory Policy Board and the NLETS Board of Directors.

USER agrees to abide by the conditions set forth in the primary "USER AGREEMENT AND SYSTEM RESPONSIBILITIES OF THE TERMINAL AGENCY."

SLED reserves the right to immediately suspend furnishing data to USER when either the security or dissemination requirements approved by either the NCIC Advisory Policy Board or the NLETS Board of Directors and adopted by SLED CJIS (SCIC), NCIC and NLETS are violated. SLED may reinstate the furnishing of data in such instance upon receipt of satisfactory assurance that such violation has been corrected.

Liability for Dissemination

User shall record all dissemination's of Criminal History Records Information (CHRI) obtained from the SLED CJIS through the servicing agency referred to in this Agreement as the Terminal Agency. Such log will reflect the name to the requestor, the authority of the requestor, the purpose of the request, the case number, the identity of the individual to whom the information relates, dissemination, employee and the date of the dissemination. Such log shall be maintained and retained for twelve (12) months from the date of release. USER must assure that CHRI received from SLED CJIS will only be used for those purposes for which it was provided.

Date _____

AGENCY SERVICED

Signature-Authorized Representative

Typed/Printed Name

Title

Address (Street, City, Zip)

Phone

SERVICING AGENCY

Signature - Authorized Representative

Typed/Printed Name

Title

Address (Street, City, Zip)

Phone

DISCIPLINARY POLICY

VIOLATION	1 ST OFFENSE	2 ND OFFENSE	3 RD OFFENSE
Unauthorized disclosure or receipt of SLED/CJIS - FBI/NCIC criminal justice information	2 - 5 days suspension to dismissal	5 - 10 days suspension to dismissal	15 days suspension to dismissal
Release of drivers license or vehicle registration information to other than criminal justice employees	2 - 5 days suspension	5 - 10 days suspension	15 days suspension to dismissal
Release of information to private security guards or firefighters	2 - 5 days suspension	5 - 10 days suspension	15 days suspension to dismissal
Allowing the use of the system by personnel not certified by SLED, except for job training toward certification.	3 days suspension to dismissal	5 days suspension or dismissal	Dismissal
Failure to comply with policies and procedures established in the XXX PD and SLED/CJIS-FBI/NCIC Operations and Procedures Manual.	Written reprimand to 3 days suspension	3 - 5 days suspension	5 days suspension or dismissal
Failure to log information supplied to the Coroner's office, the Solicitor's office, or any other criminal justice employee who does not have a user agreement with XXX PD.	Written reprimand To 3 days suspension	3 - 5 days suspension	5 days suspension or dismissal
Unauthorized modification or destruction of system data; loss of computer system processing capability	3 days suspension to dismissal	5 - 10 days suspension or dismissal	15 day suspension to dismissal
Loss by theft of any computer system media including: chip ROM memory, optical or magnetic storage medium, hard copy printout, etc.	3 days suspension to dismissal	5 - 10 days suspension or dismissal	15 day suspension to dismissal
Improper recordkeeping	Oral reprimand To 3 days suspension	1 - 3 days suspension	3 days suspension or dismissal

Validation and Quality Control

Validation minimizes an agency's involvement in litigation because of inaccurate, incomplete and untimely information that was entered into the SLED/CJICS and/or FBI NCIC files. Validation is an examination by an originating agency of its active records in SLED/CJICS and FBI/NCIC to determine what records should remain active. What records should be modified. What records should be cancelled.

It shall be the responsibility of the Chief Administrative Officer of each terminal agency in the CJICS System to designate, in a formal manner, a Terminal Agency Coordinator, and an Assistant Terminal Agency Coordinator, pursuant to FBI/NCIC policy. The TAC or ATAC shall be responsible for the agency's validation program.

General responsibilities of the validation position are inclusive of, but not limited to:

- A. Ensuring that appropriate validation documentation is on file for all records entered.
- B. All records on the Validation Printout are to be test queried, and the response shall be compared to the original source document.
- C. A record of all record entries and modifications shall be maintained as part of the original source document.
- D. Contact the original source of the case report by phone: Complainant, Court, Insurance Company, and/or Parent.
- E. If unable to make contact with or obtain a positive response from the record source, cancel the record unless a law enforcement supervisor feels that this is an active case and requests that the case remains active in NCIC. If this is the case, documentation should be kept on file showing why the record was not cancelled. This information should include who made the request and the reason for keeping the record active.
- F. After all records have been validated, it is the responsibility of the TAC or ATAC to have the validation letter signed by the department head, and returned to SLED within 30 days.

procedures to ensure that all records in NCIC 2000 are kept accurate, complete, and up-to-date.

1. **Serious Errors**

1. In cases of serious errors, FBI CJIS will cancel the record and transmit a \$.E. administrative message to the entering agency. The \$.E. message provides the entire canceled record and a detailed explanation of the reason for cancellation.

"The law enforcement supervisor

2. Feels that this is an active case and the record should remain in NCIC."

user's
cedures
2000
s, and

2000

mail a
of the
ord so
by FBI

CJIS.

3.4 **VALIDATION**

1. Validation obliges the ORI to confirm that the record is complete, accurate, and still outstanding or active. Validation is accomplished by reviewing the original entry and current supporting documents, and by recent consultation with any appropriate complainant, victim, prosecutor, court, or other appropriate source or individual. In the event the ORI is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority must make a determination based on the best information and knowledge available whether or not to retain the original entry in the file.
2. Each month, CTAs receive a file of records to be validated. The CTAs in turn distribute the records to be validated to the ORIs as appropriate.

The validation process is implemented in two phases in NCIC 2000:

1. During Phase 1 (extending 3 years after Initial Operational Capability- IOC), the users are expected to validate records as they did prior to NCIC 2000 implementation. One letter is used to acknowledge receipt of the validation

NCIC RECORD VALIDATION REPORT

ORI/AGENCY

DATE OF THIS VALIDATION

OFFENSE

CASE NO.

NARRATIVE

This report is a result of compliance with NCIC validation requirements.

Type of entry:

- ☐ Wanted Person ☐ Missing Person ☐ Protection Order
☐ Stolen Gun ☐ Stolen Boat ☐ Securities
☐ Stolen Vehicle ☐ Stolen Registration Plate

- ☐ The victim/complainant was contacted by ☐ telephone ☐ person ☐ mail and confirmed that the information entered into NCIC is valid and the victim/complainant can be contacted in case of locating a missing person or recovery of stolen items.
- ☐ The victim/complainant in this case **could not** be contacted and there are no new leads or information relative to this investigation. The NCIC entry **remains** in NCIC. Reason:

- ☐ The victim/complainant in this case **could not** be contacted and there are no new leads or information relative to this investigation and the NCIC entry **is cancelled and attached**.
- ☐ The person entered into NCIC as a wanted person is **confirmed as still wanted** through the courts and a valid warrant is on file at this agency.
- ☐ The protection order in NCIC is **confirmed as still active** through the courts and a valid copy is on file at the agency.
- ☐ The warrant or protection order is not valid, and the NCIC entry is **cancelled and attached**.
- ☐ RECORD CANCELLED ☐ RECORD REMAINS ACTIVE

VALIDATION OFFICER'S NAME / SIGNATURE

NCIC ENTRY QUALITY CHECK

Successfully apprehending a Wanted Person, locating a Stolen Auto, Stolen articles and Missing Persons is directly attributable to the quality of data entered into the NCIC system. For this reason, it is crucial that the required fields, as well as any miscellaneous information, be both COMPLETE and ACCURATE. FBI/NCIC regulations REQUIRE that each entry be checked by a second party.

THIS FORM MUST BE COMPLETED FOR EACH ENTRY!

NIC #	CASE #	TYPE OF RECORD
<input type="text"/>	<input type="text"/>	<input type="text"/>

	<u>ACCURACY</u>	<u>COMPLETENESS</u>
VIN #	<input type="checkbox"/>	<input type="checkbox"/>
Make	<input type="checkbox"/>	<input type="checkbox"/>
Model	<input type="checkbox"/>	<input type="checkbox"/>
Color	<input type="checkbox"/>	<input type="checkbox"/>
Other Mis. #	<input type="checkbox"/>	<input type="checkbox"/>
Date of warrant	<input type="checkbox"/>	<input type="checkbox"/>
Caution indicator	<input type="checkbox"/>	<input type="checkbox"/>
Physical description	<input type="checkbox"/>	<input type="checkbox"/>
Clothing description	<input type="checkbox"/>	<input type="checkbox"/>
Known AKA's	<input type="checkbox"/>	<input type="checkbox"/>
Complete name	<input type="checkbox"/>	<input type="checkbox"/>
Extradition limitations	<input type="checkbox"/>	<input type="checkbox"/>
Correct classification (missing persons)	<input type="checkbox"/>	<input type="checkbox"/>

REVIEWED BY

DATE

ORIGINAL OPERATOR'S NAME

AFTER COMPLETING THIS FORM, PLEASE PLACE IT WITH THE CASE FILE.

*Refer to the Handout titled,
"NAC Entry Quality Check"
→ Please take a copy of it
form back to
your dept. to
make copies*

SECOND PARTY CHECK:

Tell them why they must do 2nd party checks (for accuracy, completeness)

1. A standard form has been developed to document 2nd party checks.
2. Agencies must complete this form ^{*at the time of entry*} for each Hot File entry to document that a 2nd party check has been performed.
3. Agencies will maintain the forms in their local case files for audit.
4. This will be a part of future audits.
5. This becomes effective on January 1, 1997.

Talk about the form here.

SOUTH CAROLINA LAW ENFORCEMENT DIVISION

MARK SANFORD
Governor

ROBERT M. STEWART
Chief



December 23, 2002

To: ALL Users of the SLED CJIS / FBI NCIC System

From: Lt. G.W. Hamby, SLED CJIS

Subject: **SLED Protocol for Failure to Validate NCIC Records**

As you know, the complete and timely validation of NCIC records is vital to the accuracy and utility of information in that system. Failure to completely validate NCIC records in a timely manner can have serious consequences within the law enforcement community, including civil liability for police actions taken on the basis of inaccurate or incomplete information. Unfortunately, there have been some recent instances in which persons responsible for validation of these records have not performed the duty in a timely manner. In an effort to insure the utility of the data and decrease liability, SLED CJIS has implemented the following protocol.

Please call Ms. Shameka Haskett (803-896-7208) or S/A Loui Pappas (803-896-7587) if you have questions.



An Accredited Law Enforcement Agency

P.O. Box 21398/ Columbia, South Carolina 29221-1398/ (803) 737-9000/ Fax (803) 896-7041

SLED Protocol for Failure to Validate NCIC Records

If an agency fails to return the signed validation cover sheet to SLED NCIC Training staff by the stated deadline:

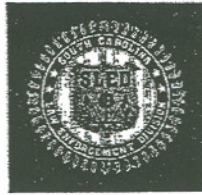
1. SLED NCIC Training staff will, within one weekday,
 - a. Send an AM message to the affected agency head, and
 - b. FAX a copy of an explanatory letter to the affected agency head, and
 - c. Mail an explanatory letter to the affected agency head, and
 - d. Notify the state Control Terminal Officer.The AM message and the letter will explain the consequences of a failure to validate NCIC records.
2. If the affected agency does not respond within two weekdays, SLED staff will telephone:
 - a. The affected agency head, or
 - b. The affected TAC.
3. If there is no satisfactory response to the telephone call, SLED NCIC staff will:
 - a. Cancel the affected NCIC records, and
 - b. Notify the Control Terminal Officer, and
 - c. Send an explanatory letter to the affected agency head.

NOTE: SLED CJIS/NCIC does not take lightly the task of canceling active NCIC records that have been entered by a law enforcement agency. The cancellation of such records can lead to serious consequences, among them **officer safety** and **citizen safety** issues. However, FBI NCIC policy is clear in its position that all records not validated by the stated deadlines must immediately be cancelled from NCIC.



An Accredited Law Enforcement Agency

P.O. Box 21398 / Columbia, South Carolina 29221-1398 / (803) 737-9000 / Fax (803) 896-7041



SLED CJIS Training
NCIC Operator Certification Program

TABLE OF CONTENTS

Introduction	1
Authorized Types of "SLED CJIS-NCIC Certification"	3
New Criteria for Candidates of SLED CJIS-NCIC Certification	5
Background Checks for NCIC Terminal Operators	6
High School Diploma or Equivalency Requirement	6
Criteria for New "NCIC Instructor" Candidates	8
Instructor Effectiveness Evaluation	10
Description and Explanation of New Forms	10
"Security Profile" Form (See Appendix A)	10
NCIC "Instructor Schedule" Form (See Appendix B)	11
"Terminal Operator ADD/MODIFY/DELETE" Form (See Appendix C)	11
Description of the "Assessment of instructor Effectiveness" Form (See Appendix D)	11
"Final -- Attendance Roster" (See Appendix E)	14
Reaffirmation Procedures	14
Transferring NCIC Certification Between Agencies	14
Procedures for Transferring CJIS-NCIC Certification	14
Procedures for Transferring CJIS-NCIC Instructor Certification	15
Closing Summary	15

Acronyms:

SLED	S.C. State Law Enforcement Division
CJIS	Criminal Justice Information Services (SLED organizational component)
NCIC.....	National Crime Information Center (National FBI program)
CSA	CJIS Systems Agencies (Designated by the FBI NCIC)
CSO	CJIS Systems Officers (Designated by the Chief of SLED)
NLETS.....	National Law Enforcement Telecommunications System
MDT	Mobile Data Terminals

Introduction

The improvements to SLED CJIS and the changes taking place with NCIC 2000 over the next few years will be unprecedented in our state's history. These changes, such as image transmission, mobile data terminals, and innovative uses of the internet will have the potential for solving more crime and making our criminal justice system more efficient and effective. These technologies have the potential for enhancing the safety of both our citizens and law enforcement officers alike. However, along with all the positive growth and technological advancements, there is a potential for greater security concerns,

MEMORANDUM

TO: All SLED CJIS-NCIC System TAC's/ATAC's

FROM: Major Carlotta C. Stackhouse
Asst. Director of SLED CJIS/NCIC CSO

RE: Modification of Re-Affirmation Procedures

DATE: September 28, 2005

Modification to SLED CJIS Re-Affirmation Procedures located on page 14 of the SLED CJIS Training-NCIC Operator Certification Program Document will become effective **October 1, 2005.**

The modified policy will be that Re-Affirmation, which includes testing, must be completed every two (2) years by or on the last date of reaffirmation for the current NCIC operator or the date of certification for NCIC new operators.

If Re-Affirmation is not completed by the stated deadline, the individual(s) operator's sign on and password will be deactivated, denying access to SLED CJIS and associated systems (SCDMV, NLETS, CPIC & NCIC). The TAC, ATAC, or terminal operator will be given thirty (30) days from the initial last date of expiration to successfully complete the reaffirmation process (individual testing on NexText Program). If the TAC, ATAC, or terminal operator does not complete his/her Re-Affirmation testing within this time frame, the TAC, ATAC, or terminal operator will have to successfully complete the appropriate certification level course (16 or 40 hours) before they will be given access to the SLED CJIS network.

In the instance of extenuating circumstances such as military duty, extended medical leave, etc, and the deadline can not obviously be met, the agency TAC must submit a written request for an extension.

If there is a need for further clarification to this process, please contact S/A Loui Pappas @ 803-896-7587 or Shameka Haskett @ 803-896-7208.

**SLED CJIS-NCIC Certification
TERMINAL OPERATOR ADD/MODIFY/DELETE FORM**

SC State Law Enforcement Division
PO Box 21398
Columbia, S.C. 29221-1398
Attention: CJIS Quality Assurance
FAX: (803) 896-7022/7218

- ☐ ADD Certified Operator (New Employee)
☐ MODIFY Operator's Record (Name, etc.)
☐ DELETE Cert. Operator (No longer employed)

From: _____ Agency: _____
(TAC or Asst. TAC) ORI: _____

Certified Operator Name:

LAST _____, FIRST _____ MIDDLE _____

Level NCIC Certification: ☐ 16-Hour; ☐ 40-Hour; ☐ Specific Skills; ☐ Instructor

Social Security #: _____ - _____ - _____ DOB: _____

☐ **ADD (New Employee):**

Did former agency submit original of completed and signed "Security Profile" form?

☐ Yes; ☐ No

Certified Operator has not been more than 30 days since last criminal justice employment.

☐ Yes; ☐ No

Has there been a criminal history completed through NCIC and NLETS in the past two years on the operator? ☐ Yes; ☐ No

(If "NO" to any of the above, a new "Security Profile" must be completed, keep the original, and submit a copy to SLED CJIS Quality Assurance)

☐ **MODIFY NCIC Certification Records:**

☐ NAME: FROM _____
TO _____

☐ Other Modification - Comments: _____

☐ **DELETE NCIC Operator from this agency.**

Did Certified Operator transfer to another S.C. criminal justice agency? ☐ Yes; ☐ No

(If yes, please provide name and ORI of agency: _____)

TAC or ALT. TAC SIGNATURE: _____

DATE: _____

SLED CJIS Training Section: _____

SOUTH CAROLINA LAW ENFORCEMENT DIVISION

MARK SANFORD
Governor



ROBERT M. STEWART
Chief

Date: August 15, 2005

To: All TACs and ATACs

From: Milton Wilmesherr, Jr.
SLED CJIS

RE: Using Purpose Code "J" for the two year reaffirmations

According to Mrs. Evelyn Proctor, FBI CJIS III/ Criminal History Section (on 8-12-05), Steve Kovol, Supervisor FBI CJIS Audit Section, Brian Episcopo and Justin Cook, FBI CJIS Senior Auditors, and FBI CJIS Auditor Jackie Ware (all on 8-15-05), Purpose Code "J" should be used for initial inquiry of a person being hired as an operator/dispatcher AND each time after that during reaffirmation, which in South Carolina, is every two years.



An Accredited Law Enforcement Agency

P.O. Box 21398 / Columbia, South Carolina 29221-1398 / (803) 737-9000 / Fax (803) 896-7041

TOUs are also available via the Internet on the Law Enforcement OnLine (LEO) at www.leo.gov, concerning access to the LEO should contact the LEO Program Office at (202) 324-8833.

SECTION 2 -- SYSTEM CHANGES

2.1 CHANGE TO NCIC ENTRY CRITERIA TO INCLUDE NONSERIOUS AND MISDEMEANOR OFFENSES

AFFECTED BY CHANGE:

Introduction
Boat File
Foreign Fugitive File
Identity Theft File
Immigration Violator File
Missing Person File
Other Transactions
Protection Order File
Convicted Sexual Offender Registry File
Supervised Release File
USSS Protective File
Vehicle File
Violent Gang and Terrorist Organization

Wanted Person File

File

EFFECTIVE DATE:

September 3, 2006

Background

In December 2003, the CJIS Advisory Policy Board (APB) approved expanding the entry criteria for the Wanted Person File of the NCIC to include nonserious misdemeanor offenses, regardless of the extradition status or the seriousness of the offense. The CJIS APB also stipulated that the NCIC System use the Extradition Limitation (EXL) Field to filter responses. Therefore, the EXL Field will be required for entry of all nonextraditable misdemeanor offenses. CJIS Division staff will create codes for the EXL Field to distinguish between misdemeanor and felony warrants.

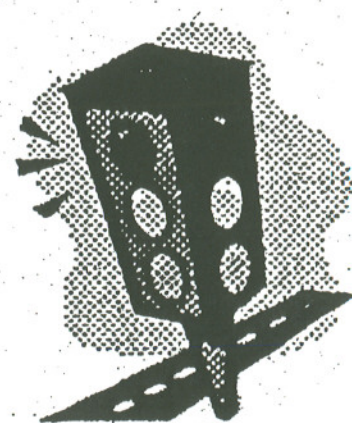
Allowing law enforcement agencies to enter nonserious misdemeanor warrant information will enhance the general search capabilities of the Wanted Person File. This enhancement will be implemented through the use of new inquiry Message Keys (MKEs), in addition to the current Wanted Person Inquiry (QW). The NCIC will return new response caveats with each corresponding inquiry MKE.

Upon entry of a nonserious misdemeanor warrant into the NCIC Wanted Person File, the entering agency should use existing codes for the Offense Field as outlined in the Uniform Offense Codes, *NCIC 2000 Code Manual* (December 2000). The entering agency should use the code that best identifies the offense (e.g., driving without a license - 5499 - traffic offense).

When an appropriate code does not exist, users should contact the CJIS Division's Investigative and Operational Assistance Unit at (304) 625-3000 for assistance in proper coding or to establish new

What Federally Prohibits an Individual From Purchasing/Receiving A Firearm?

- **Convicted of a crime punishable by imprisonment for a term exceeding one year;**
- **Fugitives from Justice - the subject of an active warrant;**
- **Unlawful Users of or Addicted to any controlled substance;**
- **Adjudicated as a Mental Defective or involuntarily committed to any mental institution;**
- **Illegal or Unlawful Aliens;**
- **Dishonorable Discharge from the U.S. Armed Forces;**
- **Renunciation of U.S. Citizenship;**
- **Subjects of Protection/Restraining Orders;**
- **Misdemeanor Crimes of Domestic Violence; and**
- **Under Information/Indictment for a crime punishable by imprisonment for a term exceeding one year.**



MessageFrom: ALDRIDGE, THOMAS G. (CJIS) (FBI)
Sent: Friday, September 23, 2005 1:02 PM
To: CARLILE, HARRY E. (CJIS) (FBI); MANSON, DEAN R. (CJIS) (FBI)
Cc: SUNDIN, M MCINTYRE (CJIS) (FBI)
Subject: Entry of civil warrants into NCIC Wanted Person File

UNCLASSIFIED
NON-RECORD

Harry & Dean,

This responds to your questions regarding the entry of civil warrants into NCIC. There is no legal objection to the entry of civil warrants into the NCIC Wanted Person File, provided the offense is extraditable. The NCIC 2000 Operating Manual does not distinguish between a civil or criminal warrant. Rather, the applicable criteria for entry of an individual (including a juvenile who will be tried as an adult) into the NCIC Wanted Person File is that the agency have an outstanding felony or serious misdemeanor warrant. The "seriousness" requirement mandates that the warrant be for something greater than a petty matter (such as vagrancy, routine traffic violations, loitering, etc.). The determination of whether a crime is a serious misdemeanor is left to the discretion of the entering agency based upon the jurisdiction's applicable law. In situations where an agency is absolutely certain that an individual wanted for a felony will not be extradited, the individual's record may still be entered in NCIC using the appropriate code in the Extradition Limitation Field.

You should be aware that the CJIS Division Advisory Policy Board approved the entry of all warrants into NCIC regardless of extradition and the seriousness of the offense. This recommendation was approved by the FBI and the NCIC enhancement is slated to be effective in September 2006. The NCIC 2000 Operating Manual is in the process of being amended to reflect this change. When this enhancement becomes effective, the NCIC user must be able to enter an appropriate code in the Extradition Limitations Field prior to entry of nonserious or nonextraditable misdemeanor warrants. Not all states or agencies may choose to enter this expanded category of misdemeanor warrants.

If you have any further questions on this matter, please feel free to contact me.

Thomas G. Aldridge
Office of the General Counsel
CJIS/Access Integrity Unit
Voice (304) 625-3620
Pager 1-877-364-5587
Cell (304) 672-0466

UNCLASSIFIED

EFFECTIVE DATE: Immediate

(June 23, 2003)

Background

At its June 2002 meeting, the CJIS Advisory Policy Board approved a proposal to modify the terminology within the *CJIS Security Policy* and the *NCIC 2000 Operating Manual* (December 1999) regarding the III logging policy. The proposed changes were based on comments from law enforcement users and recommendations from the FBI CJIS Audit Unit staff. The approved changes to the logging policy are intended to 1) accurately and clearly identify the recipient of III data and when appropriate, secondary recipients of III records and 2) provide an audit trail for local, state, and federal agencies to ensure proper logging in the III. Agencies must be able to identify the individual requester and/or secondary recipient of the III data through the unique identifier captured on the log.

Additions to the *NCIC 2000 Operating Manual* (December 1999) are indicated by highlighting, and deletions are indicated by ~~strikeout~~.

SECTION 1 -- SECURITY AND CONFIDENTIALITY

SECURITY AND CONFIDENTIALITY OF CRIMINAL HISTORY RECORD INFORMATION OBTAINED VIA THE III

Authorization to obtain records via the Interstate Identification Index (III) is governed by federal laws and state statutes approved by the U.S. Attorney General which are applicable to the U.S. Department of Justice, Federal Bureau of Investigation, and the National Crime Information Center (NCIC 2000).

Operators shall use the terminal only for those purposes which are authorized.

Copies of III data obtained from terminal devices must be afforded security to prevent any unauthorized access to or use of the data.

III records shall be maintained in a secure records environment. Such storage of records may be for extended periods only when the III records are key elements for the integrity/utility of the case files/criminal record files in which they are retained.

When retention of III records is no longer required, final destruction shall be accomplished in a secure manner so as to preclude unauthorized access/use.

III records should be properly destroyed when the record is no longer current. Because additions or deletions may be made at any time, a new copy should be requested when needed for subsequent use.

The III shall not be used to access a record to be reviewed and/or challenged by the subject of the record. Record requests for this purpose must be submitted in writing either to the FBI Criminal Justice Information Services (CJIS) Division or to the state of record.

The Control Terminal Agency (CTA) shall ensure that all NCIC hot file transactions and III transactions (both Criminal History Inquiry [QH] and Criminal Record Request [QR]) originating from access terminal devices that access NCIC the III through the state system shall be maintained on an automated log. The hot file portion of this log must ~~shall~~ be maintained for a minimum of six months, and the III portion must be maintained for a minimum of one year. The ~~this~~ automated log must clearly ~~shall, in some way,~~ identify the operator ~~individual initiating each~~ of the III transactions, as well as the agency

should be entered as part of the message key code; for example, EG-P translates as STOLEN GUN - HOLD FOR LATENTS, and ~~EFG-P~~EFGP translates as FELONY GUN-HOLD FOR LATENTS.

SECTION 3.3 -- MESSAGE FIELD CODES FOR MODIFICATION

FIELD NAME	REQUIREMENTS	MESSAGE FIELD CODE	FIELD LENGTH	DATA
HEADER	MANDATORY	HDR	9-19	ALPHABETIC, NU SPECIAL CHARA
MESSAGE KEY	MANDATORY	MKE	2-2 2-3	ALPHABETIC
ORIGINATING AGENCY IDENTIFIER	MANDATORY	ORI	9-9	ALPHABETIC, NU
NCIC NUMBER	CONDITIONAL	NIC	10-10 1-11	ALPHABETIC, NU
SERIAL NUMBER	CONDITIONAL	SER	1-20*	ALPHABETIC, NU
ORIGINATING AGENCY CASE NUMBER	CONDITIONAL*	OCA	1-9 1-20*	ALPHABETIC, NU SPECIAL CHARAC
NAME OF VALIDATOR	OPTIONAL	VLN*	1-30	ALPHABETIC, NU SPECIAL CHARAC
ANY FIELD(S) FROM ENTRY TRANSACTION				

*NCIC 2000 format only

SECTION 4.3 -- MESSAGE FIELD CODES FOR CANCELLATION

FIELD NAME	REQUIREMENTS	MESSAGE FIELD CODE	FIELD LENGTH	DATA TYPE
HEADER	MANDATORY	HDR	9-19	ALPHABETIC, NUMERIC, SPECIAL CHARACTERS
MESSAGE KEY	MANDATORY	MKE	2-2 2-3	ALPHABETIC
ORIGINATING AGENCY IDENTIFIER	MANDATORY	ORI	9-9	ALPHABETIC, NUMERIC
NCIC NUMBER	CONDITIONAL	NIC	10-10 1-11	ALPHABETIC, NUMERIC
SERIAL NUMBER	CONDITIONAL	SER	1-20*	ALPHABETIC, NUMERIC
ORIGINATING AGENCY CASE NUMBER	MANDATORY	OCA	1-9 1-20*	ALPHABETIC, NUMERIC, SPECIAL CHARACTERS
DATE OF CANCEL	MANDATORY	DOC	8-8	NUMERIC
REASON FOR PROPERTY RECORD REMOVAL	OPTIONAL	RPP*	10-21	ALPHABETIC, NUMERIC

*NCIC 2000 format only

2.6 POLICY CHANGE THAT REQUIRES LOCAL AGENCIES TO LOG THE INDIVIDUAL REQUESTER AND/OR SECONDARY RECIPIENT OF INTERSTATE IDENTIFICATION INDEX (III) RECORDS USING A UNIQUE IDENTIFIER

AFFECTED BY CHANGE: Interstate Identification Index

authorizing all the transactions. III logs must ~~shall~~ also, in some way clearly identify the requester and secondary recipient. ~~record recipient.~~ The unique identification on the log must take the form of a unique identifier that must be unique to the individual requester and the secondary recipient throughout the minimum one-year retention period. ~~This information can be captured at log on and can be a name, badge number, serial number, or other unique identifier.~~

2.7 NCIC 2000 OPERATING MANUAL POLICY ADDITION TO COINCIDE WITH THE CJIS SECURITY POLICY REQUIREMENT THAT AGENCIES PROVIDE REASONS FOR INTERSTATE IDENTIFICATION INDEX (III) INQUIRIES

AFFECTED BY CHANGE: **Interstate Identification Index**

EFFECTIVE DATE: **Immediate**

Background

At its June 2001 meeting, the CJIS Advisory Policy Board (APB) approved a proposal to modify the terminology within the *CJIS Security Policy* regarding the use of III information. The proposed changes were based on recommendations from law enforcement users and a consensus of the APB membership. The approved changes to the Use of Information policy are intended to 1) ensure that agencies can accurately and clearly identify the reason for each III inquiry and 2) provide an audit trail for local, state, and federal agencies to ensure authorized III use.

Additions to the *NCIC 2000 Operating Manual* (December 1999) are indicated by highlighting, and deletions are indicated by ~~strikeout~~.

INTERSTATE IDENTIFICATION INDEX (III)

SECTION 2.1 -- SYSTEM OVERVIEW

4. The Privacy Act of 1974 requires the FBI to maintain an audit trail of the purpose of each disclosure of a criminal history record and the recipient of that record. Therefore, inquiries and record requests transmitted to III must include the purpose for which the information is to be used. The purposes for which certain agencies may use III and the appropriate codes for use are the following:

Code	Agency	Purpose
C	Criminal Justice	Used for official duties in connection with the administration of criminal justice.
Code	Agency	Purpose
J	Criminal Justice Employment	Used when the III transaction involves employment with a criminal justice agency or the screening of employees of other agencies over which the criminal justice agency maintains management control. Criminal justice employment has been separated from other criminal justice purposes due to the requirement of some state agencies participating in III. For those states that are unable to provide a record for a purpose code J inquiry (i.e., state statute), the FBI will provide the record on-line.
I	Interstate-approved	Used when the III transaction involves noncriminal justice employment and/or licensing. Limited to one agency in each state with approved state

SOUTH CAROLINA LAW ENFORCEMENT DIVISION

JIM H. HODGES
Governor



ROBERT M. STEWART
Chief

Memorandum

March 26, 2001

TO: Sheriffs, Chiefs and Other CJIS Network Users
FROM: Major Mark Huguley *Mark Huguley*
RE: NCIC / CHRI Authorized Users

Enclosed, please find a copy of a memorandum from Judge Manuel L. Real, Chairman of the FBI CJIS Advisory Policy Board Sanctions Subcommittee. Judge has directed that each CTO disseminate this letter to all NCIC users and obtain an acknowledgement.

As the agency head for your department, both you and your Terminal Agency Coordinator (TAC) should sign below and return this acknowledgement by April 15, 2001. In addition, please copy and disseminate Judge Real's letter to all persons in your department who use NCIC. Your assistance is appreciated and important to ensure continued NCIC access.

I acknowledge receipt and review of the memorandum dated March 8, 2001, from Judge Manuel L. Real to "All Control Terminal Operators and Federal Service Providers" addressing misuse of NCIC / criminal history record information.

NAME OF DEPARTMENT: _____ ORI: _____

Print Name of Agency Head: _____

E-mail Address: _____

Signature of Agency Head: _____ Date: _____

Print Name of TAC: _____

Signature of TAC: _____ Date: _____

E-mail Address: _____

A POSTAGE PAID SELF-ADDRESSED ENVELOPE IS ENCLOSED FOR RETURN.



SOUTH CAROLINA LAW ENFORCEMENT DIVISION



JIM HODGES
Governor

ROBERT M. STEWART
Chief

March 30, 2001

Honorable Manuel L. Real
Chairman
Ad Hoc Sanctions Subcommittee
CJIS Advisory Policy Board
312 North Spring Street, Room 217-P
Los Angeles, CA 90012

Dear Judge Real:

In reference to your letter of March 8, 2001, to Control Terminal Operators and Federal Service Coordinators regarding misuse of the NCIC and CHRI, please be advised that the South Carolina Law Enforcement Division has taken the requested action.

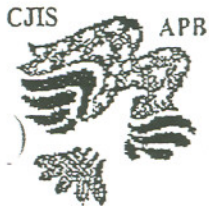
Your letter was furnished to all Sheriffs, Chiefs of Police and other CJIS network users in South Carolina. Each recipient was asked to sign and return a cover memorandum acknowledging receipt and review of your letter. In addition, each recipient was asked to copy and disseminate your letter to all NCIC users within their span of authority.

Your attention to the subject of misuse is appreciated. Should you have any questions, please feel free to contact me at 803-896-7142. With best regards, I am

Very truly yours,

Major Mark Huguley
Assistant Director





CJIS ADVISORY POLICY BOARD
AD HOC SANCTIONS SUBCOMMITTEE

Judge Manuel L. Real, Chairman
312 North Spring Street, Room 217-P
Los Angeles, California 90012

TELEPHONE:
(213) 894-5267

March 8, 2001

TO: All Control Terminal Operators and Federal Service Coordinators

With the recent increase of reports and other allegations of misuse of the Interstate Identification Index (III), and one instance of indictment by a Federal Grand Jury of a County Sheriff for alleged misuse of the III, the following information is being furnished as a reminder of proper and authorized uses of this system.

As you are aware, the III is an automated system which facilitates the interstate exchange of on-line criminal history record information (CHRI) between criminal justice agencies. It consists of an index containing individuals' names, aliases, physical descriptors, identifying numbers, fingerprint classifications, and the names of the agencies maintaining the criminal history information. It is accessed via the National Crime Information Center (NCIC) by insertion of name and other personal descriptors. There are currently 41 states participating in the III system, with approximately 33 million records available. Over 183,000 queries of the III are made daily.

The United States Department of Justice and federal courts have interpreted Title 28, United States Code (U.S.C.), Section 534 (the basic and fundamental authorization for the collection, acquisition, exchange and dissemination of CHRI) to require restricted access to FBI CHRI to criminal justice agencies for criminal justice purposes and to federal agencies authorized to receive it pursuant to a federal statute or executive order.

Title 28, Code of Federal Regulations, Part 20, 3(g), defines "criminal justice agency" as "(1) Courts; [or] (2) a governmental agency or any subunit thereof which performs the administration of criminal justice pursuant to a statute or executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice." Section 20.3(b) defines the term "administration of criminal justice" by stating that "the administration of criminal justice means performance of any of the following activities: Detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders."

TO: All Control Terminal Operators and Federal Service Coordinators
March 8, 2001
Page 2


The Privacy Act of 1974 and the Computer Fraud and Abuse Act of 1986 are two federal statutes affording criminal and civil liability for violations of privacy and security provisions relating to the use of CHRI. Additionally, 28 U.S.C., Section 534, contains provisions calling for the cancellation of access rights by criminal justice agencies if the dissemination of CHRI is made outside the receiving department or a related agency. Furthermore, most (if not all), states have laws which criminalize or provide civil liability for misuse/unauthorized dissemination of CHRI.

In the case of the County Sheriff alluded to above, the III was used to disqualify voters who voted against the incumbent Sheriff. The prosecution alleged that the Sheriff misused the III by disqualifying voters who voted against him, and that such use was not in conjunction with an official criminal investigation (as the Sheriff alleged), but merely for the personal use of the Sheriff in an attempt to maintain his elected office. Although state law did in fact disqualify persons from voting based upon certain types of convictions, the government alleged that only after word spread of the Sheriff's use of the III to disqualify those voters who voted against him did he claim that a criminal investigation had been initiated. The election was extremely close, with the winner (who was not the incumbent/defendant) winning by only several dozen votes. With the post election disqualification of voters (based upon the III results), the state's highest court removed the new Sheriff and declared the incumbent/defendant the winner. During trial in the United States District Court, the defendant Sheriff alleged successfully that discovery infractions had prejudiced his ability to defend himself. The United States District Court ruled for the Defendant and dismissed the case. The government appealed this decision.

While not frequent, criminal prosecutions for III misuse do occur, whether based upon federal law or state law. The FBI's Criminal Justice Information Services Division, Access Integrity Unit is currently researching the feasibility of obtaining federal law specifically addressing III misuse, rather than relying on generic computer or electronic access device classifications as the foundation for prosecution.

Among some of the more common examples of III misuse are the following: licensing and employment backgrounding for teachers, salesmen, gaming industry personnel and volunteers working with children, the elderly and the disabled.

Users are again reminded that, with the exception of federally approved uses such as the National Instant Criminal Background Check System, the Security Clearance Information Act, the pilot project under the Housing Opportunity Program Extension Act and the emergency placement of children recently authorized by the Compact Council (which



TO: All Control Terminal Operators and Federal Service Coordinators

March 8, 2001

Page 3

requires submission of fingerprints within a 5 day period), the III may only be accessed and used by criminal justice agencies for criminal justice purposes. Users are also reminded that III may be used for criminal justice employment backgrounding, but that such inquiry should be followed up with a fingerprint submission.

I am requesting that you provide this information regarding authorized uses and dissemination of CHRI to users of your Control Terminal Agency system. It is imperative that each user of the III acknowledge in some manner their receipt of this information and accept responsibility and potential consequences that could be imposed for misuse. Please provide a written response to me by April 9, 2001 on how you will achieve the dissemination and acknowledgment of this information by all of your users. If you have questions regarding this request, please contact Ms. Robin Stark, Unit Chief, CJIS Audit Unit, (304) 625-2941. I appreciate your continued efforts to reduce misuse of the III.

Sincerely,



Manuel L. Real
Chairman
Ad Hoc Sanctions Subcommittee
CJIS Advisory Policy Board

- 1 - Mr. William C. Temple, FBI
- 1 - Mr. Tom Bush, FBI
- 1 - Mr. Roy G. Weise, FBI
- 1 - Mr. Cal Sieg, FBI
- 1 - Ms. Robin A. Stark, FBI

SOUTH CAROLINA LAW ENFORCEMENT DIVISION

MARK SANFORD
Governor



ROBERT M. STEWART
Chief

DATE: April 16, 2004

TO: All Users of the SLED CJIS/ FBI NCIC System

FROM: MAJ Mark W. Huguley
Assistant Director for CJIS

Subject: The Use of Authorized Purpose Codes

Accompanying this cover sheet, please find a copy of the five-page listing of authorized purpose codes and their uses.

Listed first are the FBI Interstate Identification Index (III) Purpose Codes, followed by the South Carolina Criminal History Purpose Codes.

Please keep this purpose code listing with your FBI NCIC 2000 Manual and your SLED CJIS Operations Manual so individuals (operators, dispatchers, TACs and ATACs, etc.) may make reference.



An Accredited Law Enforcement Agency



The following are the current Purpose Codes and their Purpose:
(*FBI Policy is in italics*)

Interstate Identification Index (III)

Code	Agency	Purpose
C	<i>Criminal Justice</i>	<p><i>Used for official duties in connection with the administration of criminal justice. If Purpose Code C is used, the JUS field must contain a specific reason (e.g., "narcotic investigation", "traffic investigation", "prisoner classification", "probation screening" as well as a case number if possible).</i></p> <p><i>Some examples of authorized uses:</i></p> <ol style="list-style-type: none"><i>(1) Vendors or contractors at criminal justice agencies who are NOT involved with the actual administration of criminal justice at the criminal justice agency, e.g., carpet cleaners, individuals responsible for maintaining vending machines, janitors cooks, etc.</i><i>(2) Volunteers at the criminal justice agency who are NOT involved with the actual administration of criminal justice at the criminal justice agency, e.g., participants in the community ride-along programs, volunteers at a confinement facility who are providing social or community services rather than rehabilitative services, etc.</i><i>(3) Confinement facility visitors.</i><i>(4) Inmates of a confinement facility.</i><i>(5) Inmate's mailing list.</i><i>(6) "Contract employees" working within a federal office, a federal facility site or a federal courthouse building.</i> <p><i>These checks <u>must</u> be followed by submission of fingerprints to the FBI.</i></p> <ol style="list-style-type: none"><i>(7) The solicitor's office may conduct background checks on witnesses, victims and jurors.</i>

C	Criminal Justice	<p>(8) Candidates for state judicial office <u>if the court performs the administration of criminal justice</u>. Conversely, candidates for appointment as "civil-side" judges would <u>not</u> be amenable to III.</p> <p>(CJIS/NCIC TOU 03-2; 6-23-03)</p>
J	Criminal Justice Employment	<p>Used when the III transaction involves employment with a criminal justice agency or the screening of employees of other agencies over which the criminal justice agency maintains management control. The JUS field must be filled in with a specific description of the background check with a department number if possible.</p> <p>Some examples of authorized uses:</p> <p>(1) Vendors or contractors at the criminal justice agency who ARE involved with the actual administration of criminal justice at the criminal justice agency, e.g., personnel involved with the maintenance of computer systems, upgrading records systems, data entry clerks, etc.</p> <p>(2) Volunteers at the criminal justice agency who ARE involved with the actual administration of criminal justice at the criminal justice agency, e.g., volunteer dispatchers, volunteer data entry clerks, volunteers at a confinement facility who are providing inmate rehabilitation, etc.</p> <p>(CJIS/NCIC TOU 03-2; 6-23-03)</p>
I	Interstate-approved Noncriminal Justice	<p>May <u>only</u> be used by the SLED state identification bureau- a fingerprint-based identification must precede Direct Access to III & inquiry must use an out-of-state SID or FBI number.</p>
F	Weapons-related checks	<p>Used when the III transaction involves weapons-related background checks.</p> <p>"Purpose code "F" must be used by criminal justice agencies for the purpose of (a) issuing firearms-related permits & explosives permits pursuant to state law,</p>

regulation or local ordinance; (b) returning firearms to their lawful owners; and (c) enforcing federal & state law prohibiting certain persons with criminal records from possessing firearms, in circumstances in which firearms have been pawned." (FBI CJIS Policy, Section 2.5, received 2-26-04). SLED Regulatory is authorized to use "F" when inquiring prior to issuing permits for Concealed Weapons Permits, denied firearm purchases & armed security guards. (SLED Regulatory memo, 2-6-02).

*D Domestic Violence
and Stalking*

Used by civil or criminal courts in domestic violence or stalking cases. ORIs ending in D (those issued to civil courts) are not allowed access to III for any other purpose.

Other authorized uses: Law enforcement agencies providing III records to criminal or civil courts for domestic violence hearings (This III inquiry is in reference to court use only).

H Housing

Restricted to use by SLED only.

*A Administrative File
Maintenance*

Used when the authorized participating state agency generates a III transaction for internal review. Responses for this purpose code may not be disseminated for any other reason. Response is limited to that state's portion of the record maintained by the FBI; no federal arrest data are provided.

S National Security

Used when the III transaction is generated by an agency authorized by the Security Clearance Information Act (SCIA) in investigation of individuals for access to classified information or assignment

*in sensitive national security duties.
Use restricted only to Department of
Defense (DOD); Defense Investigative
Service (DIS); The U.S. Office of
Personnel Management (OPM); the
Central Intelligence Agency (CIA);
Department of State (DOS); Department
of Transportation (DOT) and the National
Security Agency (NSA).
(Mrs. Evelyn Proctor, FBI CJIS, February
17, 2004).*

<i>V</i>	<i>Visa Applicants</i>	<i>Limited to QH inquires by the Department of State, Consolidated Immigrant Processing Visa Center.</i>
<i>X</i>	<i>Inactive</i>	<i>Requires fingerprint submission within a specified time period following direct access.</i>

South Carolina Criminal History Purpose Codes

<i>B</i>	<i>Solicitors & Summary Court Judges S.C.C.H.R.I. only</i>	<i>Restricted <u>only</u> to solicitors and summary court judges so they may determine whether a criminal history record subject has previously expunged a criminal history Record. No CHRI is disseminated and no secondary dissemination is authorized for information indicating a record was expunged, unless to the subject formerly having that record.</i>
<i>E</i>	<i>Employment or Licensing: S.C. C.H.R.I. only</i>	<i>Used by SLED for public dissemination; Used by local agencies for checking on pawn broker licenses in their jurisdiction. Department of Social Services Investigators are authorized to inquire on foster parents.</i>

The Department of Revenue is authorized to use Purpose Code E for issuing bingo licenses.

Local terminal agencies may conduct inquiries for the "Guardian Ad Litem".

Z Criminal Justice
S.C. C.H.R.I. only

Used for court-ordered, state criminal history record information for mental health evaluations. Secondary disseminations should be logged.

The use of "Z" is authorized for the release of CHRI to DSS under state statute Section 20-7-616 (the Central Registry of Child Abuse and Neglect.) Additionally, you must place the DSS requestor's name in the ATN field and place the following in the JUS field: "Central Registry of Child Abuse & Neglect, Section 20-7-616". This dissemination is to be logged on the manual dissemination log kept by your agency. No III inquiry for this purpose is authorized.

INDIVIDUAL REQUEST FOR CRIMINAL RECORD REVIEW

I. PERSONAL INFORMATION

NAME: _____

ADDRESS: _____
(STREET) (CITY) (STATE) (ZIP CODE)

TELEPHONE: _____ RACE: _____ SEX: _____ DATE OF BIRTH: _____

RECORDS CLERK: _____ DATE: _____

II. IDENTITY VERIFICATION

<p>IIa. _____ FPC-SLED/AGENCY _____ COUNSEL KNOWN BY AGENCY IDENTIFIED BY: _____ _____ OTHER: _____ FEE RECEIVED: \$ _____</p>	<p>IIb. (IF COUNSEL PRESENT) NAME: _____ ADDRESS: _____ I HEREBY CERTIFY THAT I AM DULY AUTHORIZED TO PRACTICE LAW IN THE STATE OF: _____ AND THAT I HAVE BEEN RETAINED BY: _____ _____ TO AID AND ASSIST HIM/HER IN THE REVIEW AND POSSIBLE CHALLENGE OF HIS/HER CRIMINAL HISTORY RECORD. _____ (SIGNATURE) (DATE)</p>
--	---

III. _____ I HAVE REVIEWED MY CRIMINAL HISTORY RECORD, IF ANY, AND HAVE NO CHALLENGE TO ITS CONTENTS. I HAVE RETURNED MY RECORD, IF ANY.

_____ I HAVE REVIEWED MY CRIMINAL HISTORY RECORD AND WISH TO SPECIFICALLY CHALLENGE CERTAIN ENTRIES.

_____ I HAVE ASKED FOR AND RECEIVED A COPY OF THE SPECIFIC ENTRIES I WISH TO CHALLENGE. THIS COPY WILL BE USED SOLELY FOR THE PURPOSE OF PREPARING A CHALLENGE.

_____ I DO NOT REQUIRE ANY COPIES OF ANY ENTRIES ON MY RECORD.

_____ I HAVE BEEN COMPLETELY INFORMED OF THE PROCEDURES FOR CHALLENGING MY RECORD.

_____ THE FINGERPRINT RECORD CARD USED FOR IDENTIFICATION HAS NOT BEEN RETURNED.

SIGNATURE: _____ DATE: _____

SIGNATURE: _____ DATE: _____
(OF THE RECORDS CLERK)

PUBLIC NOTICE

THE DEPARTMENT OF JUSTICE REGULATIONS (20.21)(g)(1) PROVIDE THAT ANY INDIVIDUAL SHALL, "UPON SATISFACTORY VERIFICATION OF HIS OR HER IDENTITY, BE ENTITLED TO REVIEW WITHOUT UNDUE BURDEN TO EITHER THE CRIMINAL JUSTICE AGENCY OR THE INDIVIDUAL, ANY CRIMINAL HISTORY RECORD INFORMATION MAINTAINED ABOUT THE INDIVIDUAL AND OBTAIN A COPY THEREOF WHEN NECESSARY FOR THE PURPOSE OF CHALLENGE OR CORRECTION".

VERIFICATION OF SUCH INDIVIDUAL'S IDENTITY MAY ONLY BE AFFECTED THROUGH SUBMISSION OF HIS NAME, DATE OF BIRTH, AND A SET OF ROLLED FINGERPRINTS WHICH WILL BE SUBMITTED TO THE STATE LAW ENFORCEMENT DIVISION AND AFTER RETURN OF SUCH VERIFICATION TO THIS DEPARTMENT A REVIEW OF HIS OR HER RECORD MAY BE MADE AT THE RECORDS OFFICE, BEAUFORT POLICE DEPARTMENT, MONDAY THROUGH FRIDAY, FROM 10:00 A.M. TO 4:00 P. M., EXCLUDING HOLIDAYS. THIS SERVICE MAY BE OBTAINED THROUGH THIS OFFICE WITHOUT ANY FEE BEING CHARGED AT THE PRESENT TIME. HOWEVER, THIS IS SUBJECT TO REVIEW AND IF DEEMED NECESSARY A "REASONABLE" FEE MAY BE CHARGED TO COVER ACTUAL COSTS.

REVIEW MUST BE MADE IN PERSON OR BY COUNSEL, PROVIDED THE COUNSEL HAS A FINGERPRINT CARD AND WRITTEN AUTHORIZATION OF THE PERSON REQUESTING A REVIEW. COPIES OF THE INDIVIDUAL'S RECORD SHALL BE MADE AVAILABLE TO THE INDIVIDUAL OR HIS OR HER COUNSEL ONLY FOR THE PURPOSE OF INITIATING A CHALLENGE TO THE RECORD AND ONLY THAT PORTION OF THE INDIVIDUAL'S CRIMINAL HISTORY RECORD UNDER CHALLENGE WILL BE FURNISHED.

Local Agency Policy Assessment Packet

employment with a criminal justice agency or the screening of employees of other agencies over which the criminal justice agency maintains management control. Criminal justice employment has been separated from other criminal justice purposes due to the requirement of some state agencies participating in III. For those states that are unable to provide a record for a purpose code J inquiry (i.e., state statute), the FBI will provide the record on-line. *NCIC 2000 Operating Manual, III, Section 2.1.4*

- c. Weapons-related Checks (purpose code F) - Used by criminal justice agencies for the purposes of (a) issuing firearms-related permits and explosives permits pursuant to state law, regulation, or local ordinance; (b) returning firearms to their lawful owners; and (c) enforcing federal and state law prohibiting certain persons with criminal records from possessing firearms, in circumstances in which firearms have been pawned. *NCIC Technical and Operational Update, Section 2.2.1, September 9, 2002*
- d. Domestic Violence and Stalking (purpose code D) - Used by civil or criminal courts in domestic violence or stalking cases. ORIs ending in D (those issued to civil courts) are not allowed access to III for any other purpose.
- e. Housing (purpose code H) - Used when the III inquiry is made under the authority of the Housing Opportunity Extension Act of 1996. Limited to QH inquiries. *NCIC 2000 Operating Manual, III, Section 2.1.4*
- f. Exigent Procedures (purpose code X) - For use in conducting III checks involving the emergency placement of children when unaccompanied by the immediate submission of fingerprints on the surrogate care provider(s). The purpose code X may be used by social services agencies [authorized governmental agencies, e.g., Department of Children and Family Services] authorized under an approved state statute to receive criminal history record information preceding the delayed submission of fingerprints or by law enforcement agencies servicing the record needs of such agencies. Records that have been ordered "sealed" by the state will be excluded in any response when a purpose code X is used.

In those instances where an emergency child placement occurs, the authorized governmental agency must submit a fingerprint card on the individual(s) residing in the household (as identified by the state statute) to the State Identification Bureau (SIB) within 5 business days of conducting the III name check. *NCIC Technical and Operational Update, Section 2.4, March 22, 2001*

Out Compliance: Uses purpose code "C" for "F".

**PROCEDURES FOR INDIVIDUAL RIGHT OF ACCESS AND REVIEW OF CRIMINAL
HISTORY AT THE MONCK'S CORNER POLICE DEPARTMENT**

"ANY INDIVIDUAL SHALL, UPON SATISFACTORY VERIFICATION OF HIS IDENTITY, BE ENTITLED TO REVIEW, WITHOUT UNDUE BURDEN TO EITHER THE CRIMINAL JUSTICE AGENCY OR THE INDIVIDUAL, ANY CRIMINAL HISTORY RECORD INFORMATION MAINTAINED ABOUT THE INDIVIDUAL AND OBTAIN A COPY THEREOF WHEN NECESSARY FOR THE PURPOSE OF CHALLENGE OR CORRECTION." SECTION 20, 21 (G) (1), SECURITY AND PRIVACY REG. S.

IF AT ANY TIME YOU ARE UNSURE AS TO WHAT YOU SHOULD DO-**STOP!** ASK THE CHIEF AND IF HE DOES NOT KNOW, HE WILL CALL SLED. DO NOT GIVE OUT ANY CRIMINAL RECORDS UNLESS YOU ARE SURE THAT YOU ARE DOING IT CORRECTLY.

REVIEW

IF ANY INDIVIDUAL WISHES TO REVIEW HIS/HER CRIMINAL RECORD AT THIS DEPARTMENT, FOLLOW THE FOLLOWING STEPS:

- I. HAVE HIM/HER FILL OUT THE TOP SECTION OF THE, "INDIVIDUAL REQUEST FOR CRIMINAL RECORD REVIEW," FORM. NEXT YOU SHOULD SIGN AND DATE IT.
- II. HAVE THE REQUESTOR TAKEN TO THE BOOKING DESK WHERE THEY SHOULD TAKE ONE SET OF FINGERPRINTS.
- III. TELL THE REQUESTOR THAT HIS/HER IDENTITY MUST BE VERIFIED BY SLED AND THAT YOU WILL CALL OR WRITE HIM/HER IN ____ TO ____ WEEKS TO RETURN TO REVIEW HIS/HER RECORDS.
- IV. SEND THE FINGERPRINT CARD TO SLED RECORDS DIVISION WITH A COPY OF THE REQUEST FORM. WITH A NOTATION OF WHEN THE FINGERPRINTS WERE SENT TO SLED.
- V. WHEN SLED RETURNS THE FINGERPRINT CARD WITH THE ID NUMBERS, CHECK YOUR FILES TO SEE IF YOU HAVE A RECORD.

IF SLED HAS NO FILE AND YOU DO HAVE A FILE WITH A FINGERPRINT CARD, SEND THAT INFORMATION TO SLED WITH BOTH SETS OF FINGERPRINTS.
- VI. WHEN THE FILE HAS BEEN VERIFIED OR WHEN YOU FIND YOU HAVE NO RECORD, CONTACT THE REQUESTOR TO COME IN FOR REVIEW. **DO NOT TELL THE REQUESTOR WHETHER OR NOT YOU HAVE A FILE OVER THE TELEPHONE.**
- VII. WHEN THE REQUESTOR COMES IN FOR THE REVIEW, FILL OUT THE MIDDLE SECTIONS OF THE REQUEST FORM.

IF THERE IS SOMEONE OTHER THAN HIS/HER ATTORNEY TO BE PRESENT, TYPE UP THE FOLLOWING STATEMENT AND HAVE IT SIGNED.

"I, _____, HAVE BEEN REQUESTED BY _____
TO ASSIST IN INTERPRETING THEIR CRIMINAL RECORDS."
SIGNATURE OF ASSISTOR: _____ DATE: _____
SIGNATURE OF REQUESTOR: _____ DATE: _____
SIGNATURE OF RECORDS CLERK: _____ DATE: _____

- VIII. SHOW THE REQUESTOR HIS/HER RECORD, IF ANY, IN A PRIVATE AREA. DO NOT LET THE RECORD LEAVE. SHOW ONLY CRIMINAL HISTORY RECORDS (RAP SHEET).
- IX. IF THE REQUESTOR HAS NO PROBLEM WITH THE RECORD, HAVE HIM/HER FILL OUT THE BOTTOM SECTION OF THE REQUEST FORM AND RETURN THE FILE. DO NOT GIVE ANY COPIES OF THE RECORD. IF THE REQUESTOR HAS A CHALLENGE TO THE RECORD, EXPLAIN THE CHALLENGE PROCEDURES AND GO TO CHALLENGE PROCEDURES, STEP 1.

CHALLENGE PROCEDURES

- I. IF THE INDIVIDUAL WISHES TO CHALLENGE, DETERMINE IF HE/SHE WANTS A COPY OF THAT PORTION OF THE RECORD TO BE CHALLENGED. IF SO, GIVE HIM A COPY OF ONLY THAT PART OF THE RECORD.
- II. HAVE THE CHALLENGER COMPLETE THE BOTTOM PORTION OF THE REVIEW FORM AND ATTACH A COPY OF ANY RECORDS GIVEN OUT AND FILE.
- III. WHEN THE CHALLENGER IS READY TO MAKE THE CHALLENGE, HAVE HIM/HER FILL OUT THE, "CRIMINAL HISTORY RECORD CHALLENGE," FORM. TELL THE CHALLENGER THAT HE/SHE WILL BE NOTIFIED IN ____ TO ____ WEEKS, WHEN A REVIEW HAS BEEN MADE.
- IV. THE CHALLENGE AND THE FILE WILL BE REVIEWED BY _____, AND A DECISION WILL BE MADE.
REMEMBER: THE CHALLENGER SHOULD PROVE THE ERROR, THE DEPARTMENT DOES NOT HAVE TO DEFEND ITS RECORD.
- V. CALL THE CHALLENGER AND INFORM HIM/HER OF THE DECISION. IF A CORRECTION IS TO BE MADE, GO TO STEP 13.
- VI. IF THE CHALLENGER WISHES TO APPEAL, TELL HIM THAT THE CHIEF WILL REVIEW THE RECORD AND HE/SHE WILL BE NOTIFIED IN ____ TO ____ DAYS. SEND THE CHALLENGE FORM AND THE FILE TO THE CHIEF.
- VII. CALL IN THE CHALLENGER AND INFORM HIM/HER OF THE DECISION. IF A CORRECTION IS TO BE MADE, GO TO STEP 13.
- VIII. IF THE CHALLENGER WISHES TO APPEAL THE DECISION, TELL HIM/HER THAT SLED WILL REVIEW THE REQUEST AND HE/SHE WILL BE NOTIFIED IN ____ TO ____ DAYS. SEND ALL DOCUMENTS TO SLED.
- IX. CALL IN THE CHALLENGER AND INFORM HIM/HER OF THE DECISION. IF A CORRECTION IS TO BE MADE, GO TO STEP 13.
- X. IF THE CHALLENGER WISHES TO APPEAL THE DECISION, TELL HIM/HER THAT A REVIEW WILL BE MADE BY THE CRIMINAL JUSTICE INFORMATION AND COMMUNICATIONS POLICY ADVISORY BOARD AND HE/SHE WILL BE NOTIFIED IN ____ TO ____ DAYS.
- XI. CALL IN THE CHALLENGER AND INFORM HIM/HER OF THE DECISION. IF A CORRECTION IS TO BE MADE, GO TO STEP 13.
- XII. IF THE CHALLENGER WISHES TO APPEAL THE DECISION, TELL HIM/HER THAT ALL ADMINISTRATIVE REMEDIES HAVE BEEN EXHAUSTED AND THAT HE/SHE SHOULD NOW APPEAL THROUGH THE COURTS.
- XIII. IF ANY CORRECTION IS MADE:
 - a) NOTIFY ALL AGENCIES TO WHOM YOU HAVE SENT THE INCORRECT INFORMATION (CHECK YOUR DISSIMINATION LOG).
 - b) BE SURE TO NOTIFY SLED.

CRIMINAL HISTORY RECORD CHALLENGE

I. NAME: _____

ADDRESS: _____
(STREET) (CITY) (STATE) (ZIP CODE)

TELEPHONE: _____ RACE: _____ SEX: _____ DATE OF BIRTH: _____

II. AFTER REVIEWING MY RECORDS AT THE MONCK'S CORNER POLICE DEPARTMENT I FIND CERTAIN ENTRIES TO BE IN ERROR OR INCOMPLETE AS FOLLOWS:

PART OF MY RECORD NOW READS:

CASE #: _____ OTHER I.D. #'S: _____

ARREST DATE: _____ CHARGES: _____

DISPOSITION: _____

DISPOSITION DATE: _____

III. MY RECORD SHOULD READ:

CASE #: _____ OTHER I.D. #'S: _____

ARREST DATE: _____ CHARGES: _____

DISPOSITION: _____

DISPOSITION DATE: _____

IV. BASED ON THE FOLLOWING FACTS: _____

V. I HAVE ENCLOSED A CHECK FOR \$ _____ TO COVER THE AGENCY'S COSTS.

RECEIPT NO. _____ DATE: _____

SIGNATURE: _____ DATE: _____

SIGNATURE: _____ DATE: _____

(OF THE RECORDS CLERK)

MANUAL DISSEMINATION LOG

[illegible]

Help-Notes on the FBI's
"Improper Extradition Limitation" Errors

In presenting these errors, the FBI is saying that it APPEARS that the entering agency has NOT honored the limitation (if any) that they initially put into the MIS Field.

To get this type of error from the FBI, the FBI is saying that either:

(1) The Entering or "Violating ORI" agency did NOT honor their INITIALLY stated extradition limits AND they failed to modify the MIS Field to read more restrictive something like "NOEX Beyond Surrounding Counties";

OR

[and this is more likely what happened:]

(2) The LOCATING agency mistakenly entered "NOEX" thinking it meant that extradition did not occur outside the state. In this case, the locating agency should have used "EXTR" in the EXT Field simply answering the key question "Was the person extradited?" (see below).

According the FBI Auditor Shellie Williams, since ALL South Carolina Wanted Person records are at the FBI, extradition MUST be considered JURSDICATION TO JURSDICATION (and NOT state-to-state). Even initially, if agencies are not willing to go even "statewide" (within SC), they must indicate in the MIS Field something like "NOEX Beyond Surrounding Counties" or "NOEX Beyond 50 Mile Radius."

To answer the extradition question, simple ask "Was the person extradited?" If he WAS extradited, REGARDLESS IF THE PERSON WAS EXTRADITED WITHIN THE STATE, he was still extradited and "EXTR" should be put in the EXT Field.

[illegible]

62

THIS LOG MUST BE KEPT PERMANENTLY...

For Vehicle Registration Information and Officer Safety use:

QVRQ

This Inquiry checks:

- Stolen Vehicle File
 - Vehicle Registration (owner and vehicle).
-

For Driver Registration , Driver's License Status
and Officer Safety use:

QWDQ

This Inquiry checks:

- Wanted Person File (and "Spin-Off" Files)
- Driver Registration
- Driver's License Status

For Driver History, Driver Registration, DL Status
and Officer Safety use:

QWKQ

This Inquiry checks:

- Wanted Person File (and "Spin-Off" Files)
- Driver Registration
- Driver's License Status
- Driver History

Attention and Purpose Code Required
--

When QWKQ is used to obtain Driver and Registration
Information, the following fields must be completed:

PUR – Purpose Code C
(Criminal Justice Use)

ATN – Attention Field
(Who Received and Used the Information)

SECONDARY TYPES OF DMV INQUIRIES

Search By:

- Name Only
- Name and County
- Name and Date of Birth

SOUTH CAROLINA LAW ENFORCEMENT DIVISION

MARK SANFORD
Governor



ROBERT M. STEWART
Chief

Outline for Local Agency's Written CJIS Security Policy

(For TACs only: The FBI CJIS Security Policy can be found on LEMS.Web at the bottom of the "Category List")

Your agency's written CJIS Security Policy should address all of the topics listed in the FBI CJIS Security Policy such as:

- The Distribution of the CJIS Security Policy (2.2)
- Standards of Discipline (4.2)
- Physical Security (4.4)
- Personnel Background Screening (4.5)
- Disposal of All Media (4.6)
- Technical Security (passwords, authentication, encryption, etc.) (7.0)
- Use & Dissemination of Criminal History & "Hot File" Information (8.2)



An Accredited Law Enforcement Agency

P.O. Box 21398 / Columbia, South Carolina 29221-1398 / (803) 737-9000 / Fax (803) 896-7041



MYRTLE BEACH POLICE DEPARTMENT

ADMINISTRATIVE REGULATIONS AND OPERATING PROCEDURES

Subject: *Law Enforcement Information Systems*

Number: 227

Effective Date: *January 1, 2001*

Revised Date:

Rescinds:

Dated:

Approved By:

PURPOSE

The Myrtle Beach Police Department shall adopt and abide by the guidelines from the South Carolina Law Enforcement Division for Law Enforcement Information Systems. These guidelines are written below and made a part of department regulations.

Only minor changes appropriate for our department have been made.

REGULATIONS AND OPERATING PROCEDURES FOR LAW ENFORCEMENT INFORMATION SYSTEMS

THE FOLLOWING OPERATING PROCEDURES WILL BE THE RESPONSIBILITY OF THE RECORDS SUPERVISOR, HIS/HER DESIGNEE AND ALL RECORDS EMPLOYEES. THESE POLICIES WILL BE ADHERED TO BY ALL AGENCY EMPLOYEES REGARDLESS OF POSITION.

1. **Overview: Maintaining the Records Section Filing System**

1.1 **Filing Procedures.**

The proper filing of Incident, Supplement and Arrest (booking) Reports along with criminal history records information (fingerprint cards, "rap sheets", mug shots, dispositions), and arrest warrants is vital to this agency's operation.

1.1.1 Incident and Supplement Reports will be filed in sequence by the case number. Other necessary documentation (supplements, etc.) will be filed with the incident report forming the basic case file.

1.1.2 Arrest (booking) Reports will comprise a separate file from the Incident Reports. This arrest report file will contain copies of arrest reports and will be filed under the name of each offender or the offender's identification number.

1.1.3 Juvenile Arrest Information will be filed separately from other arrests. The names of juvenile arrestees will not be disseminated outside this agency with the exception of Section 20-7-8510 of the Code of Laws of S.C., which allows the fingerprinting of juveniles convicted of violent crimes (as defined in S.C. Code of Laws 16-1-60) or of grand larceny of a motor vehicle to be transmitted to SLED. Fingerprint cards of juveniles convicted of these offenses will be sent to SLED. All information will be placed in envelope marked "confidential".

1.1.4 Records of Stolen Property that cannot be entered into NCIC (usually lacking a serial number or owner applied number) will be categorized and subcategorized according to the description of the stolen item. This file will be updated and kept current. Each record will have as a minimum: Victim name, case number, date of theft, property type, location of theft, identifying characteristics/unique identifiers, victim address and telephone number.

1.1.5 Arrest Warrants (to be served) will be maintained alphabetically as a separate file located in complaint area of police department. This procedure assures quick retrieval.

1.1.6 Criminal Fingerprint Cards will be maintained in a "short term" file. All criminal fingerprint cards (to include warrant numbers and/or uniform traffic ticket numbers listed by the charge(s)) will be forwarded to SLED within forty-eight (48) hours after arrest.

1.1.7 Disposition Reports (R-84 Forms) will also be retained in a "short term" file. Disposition reports will be sent to SLED Central Records Repository on all cases not tried in General Sessions Court. All disposition reports will show the warrant numbers and/or uniform traffic ticket numbers for all charges and must contain the final judicial disposition of each charge. Disposition reports will be sent to SLED as soon as possible after the disposition of the charge is known.

1.2 Retrieval Procedures:

Records will be available through a quick and efficient system of retrieval by knowledgeable and authorized personnel. The procedure must be fast and simple to use in order that officers and support personnel can retrieve vital documents whenever they are needed for law enforcement purposes. This procedure permits the agency to comply with federal and state laws, regulations and policies (i.e. FBI/NCIC, SLED/CJICS and UCR/NIBRS requirements).

Refinements may be made to the filing and retrieval system as experience dictates; however, the following minimum elements are required:

1. All incidents, supplements and case files must be retrievable by any and all of the following identifiers:
 - Case Number (OCA)
 - Victim Names (Persons, businesses, organizations, etc.)
 - Subject Names
 - Witness Names
 - Complainant Names
2. All arrest records (booking reports, arrest cards, rap sheets, etc.) must be retrievable by the names of the persons arrested.
3. All outstanding arrest warrants must be retrievable by the names of the subjects, and must be immediately available to the arresting officers and support personnel.
4. Copies of all warrants and incident reports pertaining active wanted persons, missing persons or stolen vehicles that are in the NCIC/SLED CJICS computer system must be available on site or immediately available to the NCIC terminal operators.

1.3 Storage, Retention and Destruction Procedures:

Records will be stored in a secure area safe from unauthorized access, theft, fire, flood or other natural or man-made disasters. Records RETENTION AND DESTRUCTION GUIDELINES are as follows:

1.3.1 Incident and Supplement Reports will be maintained in the active file for five years or until no further legal or administrative value exists whichever comes later. After that time, the reports will be archived or destroyed, subject to a review by personnel appointed by the agency head, and subject to the approval of the agency head.

1.3.2 Criminal History Records (to include "rap sheets", mug shots, fingerprint cards and final dispositions) will be retained until the death of the subject or for 75 years, whichever comes first. After that time, the reports will be archived or

destroyed, subject to a review by personnel appointed by the agency head, and subject to the approval of the agency head.

1.3.3 Juvenile Files (to include documents with name, date of birth, race, sex, vital statistics, photographs, warrants, a copy of the arrest/booking report) will be retained for a minimum of three (3) years after the subject reaches majority.

1.3.4 Case Files (to include investigative information) will be retained for thirty (30) years. After that time, the reports will be archived or destroyed, subject to a review by personnel appointed by the agency head, and subject to the approval of the agency head.

1.3.5 Arrest Warrants will be retained until the copy of the warrant is served, then forward the original to the issuing official.

1.3.6 Arrest/Booking Reports will be retained for ten (10) years. After that time, the reports will be archived or destroyed, subject to a review by personnel appointed by the agency head and subject to the approval of the agency head.

1.3.7 Uniform Traffic Collision Reports (Accident Reports) will be retained for ten (10) years. After that time, the reports will be archived or destroyed, subject to a review by personnel appointed by the agency head and subject to the approval of the agency head.

1.3.8 Traffic Tickets and Parking Tickets will be retained for ten (10) years. After that time, the reports will be archived or destroyed, subject to a review by personnel appointed by the agency head and subject to the approval of the agency head.

1.3.9 Breathalyzer Operator Test Report (BA Form) will be retained for ten (10) years. After that time, the reports will be archived or destroyed, subject to a review by personnel appointed by the agency head and subject to the approval of the agency head.

1.3.10 Personnel Training Files will be retained until no longer needed for administrative purposes. After that time, the reports will be archived or destroyed, subject to a review by personnel appointed by the agency head and subject to the approval of the agency head.

2. Operating Procedure for Criminal History Record Information (CHRI).

2.1 Definition of CHRI:

Criminal History Record Information (CHRI) means arrest (booking) reports, fingerprint cards, dispositions and data collected on adult individuals (seventeen

years of age or older) consisting of identifiable descriptors and notations of arrests, detentions, indictments, or other formal charges and dispositions.

2.2 Security of CHRI:

Access to the areas containing CHRI will be limited to only authorized personnel:

1. A notice signed by the agency head listing the authorized personnel is to be posted in plain view at the entrance to the area. Any personnel not on the access list will not be allowed in the area. Any violation will be reported to the agencies TAC Officer or the agency head immediately.

2. The area containing CHRI will be secure from unauthorized access. This area will be "manned" (or secured) by authorized personnel during office hours. After office hours and at times when the area is unattended, the area will be secured by locking windows, doors, file cabinets, etc.

3. All CHRI will be kept away from public view and/or access.

4. All computer terminals and printers having access to criminal history will not be in a position to be viewed by the public or unauthorized personnel. All terminals and printers will be turned off and locked if possible when not attended. No "pass words" or printed instructions on how to access the system will be left on or around such devices.

5. All classified information will be disposed of properly by either placing the information back in file, by shredding or by burning, etc.

6. To protect against fire, flood, wind or other natural or manmade disaster:

- Fire extinguishers must be in plain view and within easy access. They must be charged at all times;
- All personnel must be knowledgeable in the use of fire extinguishers;
- Exits will be clearly marked;
- Any potential fire or water hazard should be reported;
- A review of these procedures should take place periodically for the purpose of updating;
- In case of any violation or emergency in any of these areas, notify the records supervisor or agency head as soon as possible.

The agency head will have the authority to ensure that appropriate disciplinary action is taken whenever personnel violate security rules.

2.3 Criminal History Records:

Arrest data records become criminal history records when arrest records are filed in alphabetical sequence or in such a manner as to allow them to be easily or routinely retrieved.

1. A complete criminal history record contains:
 - Offender name, description and address;
 - Offender date of birth and social security number;
 - Any known aliases;
 - Arrest dates, charges and warrant numbers;
 - Case number(s) to cross-reference to incident reports;
 - Final dispositions and dates.

Criminal history records can be automated or maintained manually. CHRI will be maintained alphabetically by the offender's last name, and charges on any one offender will be listed in chronological sequence as they occur. CHRI must be kept complete, accurate and up-to-date at all times.

1. CHRI can include:
 - Criminal history index file;
 - Arrest (booking) reports;
 - "Rap sheets";
 - "Mug Shots";
 - Fingerprint cards;
 - Disposition reports (R-84 Forms);
 - Automated records of the above information.

2.4 Criminal Fingerprint Cards.

In order to have a criminal record at both SLED and the FBI as well as with this department, an arrested person must be fingerprinted at the time of arrest.

At least two legible sets of prints will be taken on cards approved by SLED and the FBI.

A third set of prints may be taken to be filed with his/her record at this department.

The fingerprint cards should have the agency's name, ORI number and address pre-printed by the FBI in the proper box.

Fingerprint cards will be forwarded to SLED in the pre-paid postage envelope provided by SLED. When mailing fingerprint cards and/or dispositions to SLED, check the box "Criminal Records/Fingerprints" on the front of the mailing envelope.

Fingerprint cards and dispositions must be mailed to SLED separately from other reports (i.e. UCR/NIBRS/Incident Reports, Alcohol Licensing and Enforcement, Breathalyzer Reports, Finance, etc.).

All information required on the card must be complete and accurate.

Prints that are improperly rolled, smudged or otherwise unclassifiable cannot be maintained at either SLED or the FBI and are returned to the department.

Warrant numbers or uniform traffic ticket numbers must be entered beside each charge so that final dispositions can later be accurately posted to the correct charges.

Fingerprint cards should be forwarded to SLED within forty-eight hours after arrest.

The agency should include FBI and SLED/SID numbers on the fingerprint cards if available. These numbers may be obtained from previous criminal history records or by inquiring through the SLED terminal.

2.5 Final Disposition Reports.

Final disposition reports (the R-84 Form) are essential to complete criminal history records of all Magistrate or Municipal Court cases; R-84 forms are not needed for General Sessions court cases.

The final disposition report must be filled out and completed with the fingerprint cards at the time of arrest as part of the booking process.

All disposition reports will show the warrant numbers and/or uniform traffic ticket numbers for all charges and must contain the final judicial disposition of each charge.

The disposition reports will be maintained in a "pending"-type filing status awaiting court action. As dispositions are received and posted and the report becomes complete, the original disposition report will be forwarded to SLED.

When mailing dispositions to SLED, check the box "Criminal Records/Fingerprints" on the front of the mailing envelope.

Dispositions must be mailed to SLED separately from other reports; i.e., UCR/NIBRS/Incident Reports, Alcohol Licensing and Enforcement, Breathalyzer Reports, Finance, etc.).

2.6 Mug shot Files.

Photographs of persons will be taken at the time of arrest or before the arrestee is released from custody. The photographs will be maintained in the computerized file and a copy of the photograph will be filed with the rest of the arrestee's CHRI upon request. Mug shot files are subject to expungement procedures under South Carolina State Law (S.C. Code 17-1-40; 1976 as amended).

2.7 Uniform Traffic Tickets.

The use of uniform traffic tickets by this agency will conform to The Code of Laws of South Carolina 1976, as amended, Chapter 7, Section 56-7-10 and Section 56-7-15. The use of uniform traffic tickets in criminal cases tried in Magistrate or Municipal Court requires that UCR/NIBRS arrest information (booking reports) be sent to the SLED UCR department. Officers and Records personnel will insure that appropriate reports are completed and forwarded to the SLED UCR department. These arrest reports, along with other UCR/NIBRS information, will be mailed to SLED in the pre-paid postage envelope checking the box "UCR/NIBRS/Incidents" on the front of the envelope.

2.8 Pardon Procedure.

Upon receipt of pardon documentation from the South Carolina Department of Probation, Parole and Pardon, a pardon will be added to the disposition of the record. A pardon does not constitute an expungement. South Carolina State Attorney General's Opinion number 80-86 issued to SLED on June 12, 1980, states in part that a pardon "does not establish the innocence of the person pardoned, nor does it serve to obliterate the conviction record of the pardoned offense."

A complete criminal history record with a pardon should have the following information:

- Charge;
- Date of the charge;
- Disposition and the date of the disposition;
- The pardon; and
- Date of the pardon.

2.9 Expungement Procedure.

Upon receipt of an expungement order, the following steps will be taken:

1. The order must be signed by a Circuit Court Judge (Magistrate and Municipal Court Judges lack sufficient authority to order an expungement);

2. The order must have been filed with the County Clerk of Court;
3. The order should contain consent or approval from the Circuit Solicitor;
4. The order must relate to one of the following statutory requirements for expungements:
 - a) Section 17-22-150: the defendant successfully completed the Pre-Trial Intervention Program;
 - b) Section 17-1-40: the charge was dismissed, nol prossed, not guilty, acquitted, etc.;
 - c) Section 34-11-90(e): the defendant was convicted under the Fraudulent Check Law and no additional criminal activity has taken place in one year from the date of conviction;
 - d) Section 44-53-450(b): the defendant was convicted of first offense simple possession of marijuana, received a conditional discharge and has successfully complied with the terms of that sentence;
 - e) Section 22-5-910: allows the defendant with a first offense conviction in a Magistrate's court or Municipal Court to seek an expungement.
5. As directed by the order, the arrest and booking records, mug shots and fingerprints must be destroyed; appropriate deletions must be made from other documents (incident and supplement reports, etc.). Prior to destroying, remove files and place under security for a period of two (2) weeks pending verification of record from SLED.

3. Dissemination of CHRI.

3.1 Dissemination Policy.

With limited exceptions, the documents maintained as "Criminal History Records" by this department are classified as public records.

Dissemination of these records upon request will be regulated by the SC Freedom of Information Act (FOIA) and the policy.

This agency will accept inquiries either in writing or by personal appearance. The inquiries should include information relating to the person's name, race, sex and date of birth, if available. Inquiries will not be accepted by telephone.

Records personnel will always require positive identification from the requesting individual before dissemination.

The requesting individual will complete an FOI Request Form. If the requested information is not subject to the exceptions listed in the SC FOIA (exceptions listed in Section 3.7 of this policy), then it will be disseminated upon request and compliance with Section 3.2.

Information that includes a Social Security Number or medical/health information will be marked out so it cannot be read.

If there is a question or concern regarding a specific request or the release of the information, the document request will be forwarded to the Chief's office via the chain of command for review and a final determination. The FOIA allows for a fifteen (15) day response on most FOI requests.

Records personnel will document all required information in the Manual Dissemination Log discussed below in Section 3.4. FOI Request Forms will be maintained in a separate file, alphabetized by last name.

Records personnel will suggest to the inquiring agency or individual to contact SLED Records for a more complete criminal history record in South Carolina.

3.2 Cost.

Private persons, businesses and commercial establishments or their designated representatives will be charged a fee of one dollar (\$1.00) for each criminal history record request and each copy of an incident report. The required method of payment is to be by money order, cashier's check, or company payroll check.

3.3 Hours Available For Inquiries.

Specific hours during the day that inquiries for criminal history record checks will be performed will be posted in the public lobby and at the criminal records desk.

3.4 Maintaining Manual Dissemination Logs.

Manual Dissemination Logs are required to be kept by the Code of Federal Regulations (the amendments to Chapter I of Title 28, Section 20.21 (e)) and the Code of Laws of South Carolina 1976, as amended (Chapter 73). These logs are used to document who is receiving criminal history and what information is being disseminated. The following information will be maintained in the logs in order to provide a dissemination trail:

- a. Date of dissemination
- b. Agency requestor
- c. Individual requestor
- d. Name of criminal history record subject

- e. State identification number of criminal history record subject
- f. Description of items [information] released
- g. Agency providing the information if this is indirect dissemination (information from another agency)

A record of the dissemination must be documented in the log for each inquiry made from outside this agency.

The reason for keeping this mandatory log is to insure persons who receive CHRI from this agency can be identified in case of:

- a. Improper use or dissemination; or
- b. A need to correct or update any information disseminated by this agency.

3.5 Access and Review of CHRI.

The agency will allow individuals, upon satisfactory verification of their identity, to review their criminal history record information and obtain a copy when necessary for the purposes of challenge or correction.

3.5.1 Review and Challenge Forms. The "Review" form is to be completed on the person wishing to review their record with the department. If all information is correct, the individual signs the "Review" form and the inquiry is ended.

The "Challenge" form is to be completed when the person wishes to question or challenge their record with the department. In a "challenge", it is the individual's obligation to contact the appropriate authority (the Clerk of Court or the Circuit Court Judge), and to bring the department proper documentation proving that the department's information is incorrect. Upon satisfactory documentation of an error, the Records manager will correct the challenged CHRI. The agency will then use the Manual Dissemination Log to determine if information pertaining to this particular record was disseminated to anyone within the last twelve months. If the department did disseminate this record, we will contact those agencies and advise them of the correction.

3.5.2 The "Public Notice" Displayed. Notices will be prominently displayed and will inform the public of an individual's right to inspect his/her criminal record information. The public notice, which contains rules for access, review and challenge, will cover such matters as procedures for verification of identity, the days and hours when reviews are available, locations where the reviews may be held, any fees, etc. Records personnel will be responsible for designing and posting the notices.

3.6 Controlling Case File Information.

The agency will have procedures for controlling information that may be taken out of file for official use only. The Records manager will publish such rules and design and maintain all forms required to accomplish adequate control and accountability. The number of persons authorized to access or issue documents from the files will be limited and controlled. The document logging system will include the following information:

- a. File type (case file, arrest file, etc.)
- b. Document type (incident report, supplement report, witness statement, etc.)
- c. OCA
- d. Document numbers or page numbers
- e. Date and time the documents were signed out
- f. Name of the person who signed them out (with initial or signature)
- g. Name of the person who received them (with initial or signature)
- h. Date and time the file was returned
- i. Name of the person returning the file (with initial or signature).

3.7 Release of Information Under the Freedom of Information Act.

All public documents are subject to the S.C. Freedom of Information Act (FOIA), S.C. Code of Laws 1976, as amended, Sections 30-4-10 through 30-4-100, unless specifically exempted by the act or other statutes. Law enforcement information (police records and incident reports) is considered public and must be released under the FOIA except where the release of such information will harm the agency.

1. Matters exempt from disclosure are:
 - a. The identity of informants not otherwise known;
 - b. The premature release of information to be used in a prospective law enforcement action;
 - c. The disclosure of investigatory techniques not otherwise known outside the government;
 - d. Endangering the life, health or property of any person.

Note* e. Dissemination of juvenile information.

2. The remaining information is considered public record.

The Myrtle Beach Police Department has a policy whereby the Media Liaison for the Department or designated person(s) is responsible for the review and release of law enforcement information under the S.C. Freedom of Information Act. Information may not be released to the public or news media except in conformance with the Department's Policy and Procedure.

3.8 The Dissemination of Criminal History Record Information.

The agency will obtain from the SLED/CJICS terminal the most recent criminal history record information available before any dissemination to ensure that the most accurate and up-to-date disposition data is being used (Code of Laws of South Carolina 1976, as amended, Chapter 73-22, D.).

4. Operating Procedure For Handling Uniform Crime Reports.

4.1 Incident Reports.

This agency will comply with the S.C. Code of laws 1976, as amended, Chapter 73, Section 30, which requires it "to forward all incident reports to the SLED Uniform Crime Reporting Department in response to all reports of criminal violations, regardless of the degree of seriousness of such activity and booking reports on all arrests or apprehensions regardless of the seriousness of the offense or the age of the offender."

Incident reports should be written on every criminal event reported to this agency, as well as any other events requiring law enforcement intervention; such as missing persons, runaways, suspicious fires, etc. A legible copy of the reports required by SLED will be forwarded to the UCR Section at least once a week. Reports of incidents that occur within the current month must be received at SLED no later than the fifth day of the following month. Incident reports will be screened by Supervisors and Records personnel to assure that correct and required UCR/NIBRS information is included. All reports sent to SLED must include a case number.

4.2 Supplemental Reports.

Supplemental reports will be written to modify or change the status of the reports required by SLED and to reflect additional persons involved or additional property stolen or recovered. Supplemental reports will be assigned the same case number as the original incident. Supplemental reports will be filed with the original incident report and a legible copy will be forwarded to SLED/UCR within the time frame required by SLED.

4.3 Arrest (Booking) Reports.

Arrest reports will be forwarded to SLED on all arrests or apprehensions regardless of the seriousness of the offense (excluding minor traffic offenses) or the age of the offender. Arrest reports will be assigned the same case number as the original incident. Arrest reports will be screened by Supervisors and Records personnel to assure that the correct and proper UCR/NIBRS information is included and a legible copy will be forwarded to SLED/UCR within the time frame required by SLED.

4.4 Juvenile Reports.

Even though juvenile offenders may be summoned or petitioned, or otherwise handled differently than adult offenders, juvenile arrest/apprehension reports will be sent to the SLED/UCR Department as required.

Juvenile arrest information will be filed separately from other (adult) arrests. Juvenile apprehension reports will be assigned the same case number as the original incident. The names of juvenile arrestees will not be disseminated outside the arresting agency with the exception of Section 20-7-780 of the S.C. Code of Laws, which allows the fingerprinting of juveniles convicted of violent crimes (as defined in S.C. Code of Laws Section 16-1-60) or grand larceny of a motor vehicle to be transmitted to SLED.

5. Operating Procedure For Handling Stolen Property In-house.

5.1 Stolen Property.

Stolen property cannot always be entered in the SLED/NCIC stolen property files, usually because the serial number or owner-applied number does not exist or is not available to the agency. To identify such stolen items, if they happen to be recovered, a descriptive file will be kept on each item not entered into NCIC. This file will be categorized and subcategorized to the general and then the specific description of each stolen item. Each item can be cross-referenced to an OCA or victim name.

6. Operating Procedure For Handling Arrest Warrants.

6.1 Arrest Warrants.

Arrest Warrants to be served will be maintained in a separate file located in the Complaints Section. This agency will maintain active arrest warrants in alphabetical order (by the subject's last name) so that it insures faster retrieval since the ability to produce a warrant quickly becomes important when an offender is located or apprehended. The Arrest Warrants file will be made available to all appropriate personnel. Arrest warrants are considered public record after they are served on the person charged in the warrant.

7. Operating Procedure For NCIC Matters.

THE FOLLOWING POLICIES IN SECTION SEVEN (7) WILL BE THE RESPONSIBILITY OF THE TERMINAL AGENCY COORDINATOR (TAC) OR HIS/HER DESIGNEE. THESE POLICIES WILL BE ADHERED TO BY ALL TERMINAL OPERATORS.

7.1 Terminal Operator Background Investigation-Fingerprint Check.

All prospective SLED/CJICS-FBI/NCIC terminal operators will undergo a fingerprint background check conducted by the FBI's Identification Division and SLED. One (1) blue applicant fingerprint card (Form FD-258) will be completed and sent to SLED. A background investigation will also be conducted on each prospective employee.

7.2 Certification of Agency Terminal Operators.

The FBI/NCIC policy states that all computer terminal operators employed after January 1, 1987, must achieve certification by the Control Terminal Agency (CTA), SLED, within six (6) months of employment.

Those individuals employed prior to January 1, 1987, whose assigned duties and responsibilities include the operation of the FBI/NCIC-SLED/CJICS computer terminal, must also achieve certification within a reasonable period of time as defined by the Control Terminal Officer (CTO), SLED.

SLED will be notified by letter or teletype to the attention of the South Carolina Control Terminal Officer at SLED of any changes in the status of either the Terminal Agency Coordinator (TAC) or any agency terminal operators (i.e. terminations, or name changes resulting from marriage or divorce).

7.3 The Responsibilities of the Terminal Agency Coordinator (TAC).

It shall be the responsibility of the TAC to make certain that the agency is in compliance with operator certification and reaffirmation. No person with this department is permitted to operate the SLED/NCIC Terminal without having achieved certification within the stated time frame of six months from assignment to duty as terminal operator.

The Terminal Agency Coordinator (TAC) will be appointed by the agency head. This person will attend and pass the SLED/CJICS Certification Program. This person will have authority over the duties of all terminal operators.

The responsibilities of the TAC are to handle all SLED/CJICS-FBI/NCIC matters as they might affect this agency and to ensure compliance with all SLED/CJICS-FBI/NCIC policies, rules and regulations. The TAC will serve as liaison between this agency and SLED. Coordination of all SLED/CJICS-FBI/NCIC activity as it relates to the participation of this agency will be handled through the TAC.

★ The responsibilities of the TAC will include but not be limited to:

1. Receipt of validation mailings and assurance that such validation material is processed in accordance with established standards and within the mandated time frames;

2. Making certain that all manuals and literature including newsletters relating to SLED/CJICS-FBI/NCIC are properly disseminated and posted for agency personnel to read and reference as deemed necessary;
3. Coordinate terminal operator certification and reaffirmation in accordance with programs mandated by SLED/CJICS and FBI/NCIC Advisory Policy Board;
4. Receive and ensure all changes in SLED/CJICS-FBI/NCIC policy, rules and regulations are disseminated in a timely manner, as well as ensuring all manuals, etc. are updated to reflect changes;
5. Coordinate both the SLED/CJICS mandated agency audit and any FBI/NCIC audit with the appropriate personnel from those agencies;
6. Attend seminars designed to inform the TAC of methods that will assist him/her to fulfill duties and responsibilities more effectively and efficiently;
7. Maintain User Agreements as covered and explained in section VII, C;
8. Coordinate with the enforcement units (Uniform Patrol, Investigators, Warrant Section, etc.) and the Records section to insure that documentation necessary to the initiating, clearing, canceling or confirming of a SLED/CJICS-FBI/NCIC record is properly captured and completed and that policies are in place which require and facilitate the direction of such documentation throughout the information system, especially to terminal operators.
9. The TAC is specifically required to audit five random "hot file" records per month and report in writing to the agency head any incomplete, invalid or otherwise incorrect records. The report will also specifically determine at which point in the system the errors were made (initial incident, recovery report, follow-up, warrant service, records management, terminal operations, etc.)

7.4 Discipline of SLED/CJICS-FBI/NCIC Policy Violators.

The following is the disciplinary action to be applied for violating SLED/CJICS and FBI/NCIC system policies or any laws applying to criminal justice information and communication by agency employees:

1. Unauthorized disclosure or receipt of SLED/CJICS-FBI/NCIC criminal justice information.

2. Release of driver's license or vehicle registration information to other than criminal justice employees without the Terminal Agency Coordinator's (TAC) authorization.
3. Release of information to private security guards or firefighters, without the TAC's authorization.
4. Allowing the use of the system by personnel not certified by SLED, except for job training toward certification or in special circumstances authorized by the TAC.
5. Failure to comply with the policies and procedures established in the SLED/ CJICS-FBI/NCIC Operations Manual.
6. Failure to log information supplied to the coroner's office, the solicitor's office, or any other criminal justice employee does not have a user agreement with this agency.
7. Improper record keeping.

Violation of any of the above SLED/CJICS and FBI/NCIC system policies shall be grounds for action. Referring to the "City of Myrtle Beach Personnel Policies and Procedures Manual", discipline shall be, when circumstances permit, of an increasingly progressive nature for each successive instance of employee misconduct. The recommended penalties in the manual may be modified by the appropriate City official to include a lesser or more severe penalty when extenuating circumstances are found.

Violation of any of the above SLED/CJICS and FBI/NCIC system policies shall fall under the City's Group I Offense, (q) or Group III Offense, (a).

7.5 Maintaining User Agreements.

This terminal agency is required by SLED/CJICS-FBI/NCIC to maintain a valid user agreement titled: "CRIMINAL HISTORY and CRIMINAL JUSTICE INFORMATION USER AGREEMENT." This agreement is between SLED and this agency and must be signed by the current officials of both agencies. The original is maintained at SLED and a copy must be maintained with this agency and must be available for inspection by FBI and SLED auditors.

If this agency services any non-terminal agencies, this agency and each non-terminal agency it services must maintain a separate user agreement between themselves titled: "CRIMINAL JUSTICE NON-TERMINAL ORIGINATING AGENCY IDENTIFIER (ORI) USER AUTHORIZATION AGREEMENT". This

agreement is between this agency and each non-terminal it services, and each must be signed by the current officials of each agency. The original is maintained at SLED and copies must be maintained by both this agency and non-terminal agencies and must be available for inspection by FBI and SLED auditors.

In situations where this agency services non-terminal agencies, a clearly written policy must exist outlining the duties and responsibilities of both this agency and non-terminal agencies concerning matters of NCIC and criminal history record information.

7.8 The Ten Minute Hit Confirmation Policy.

This agency adopts as its policy the procedures set forth by SLED/CJICS-FBI/NCIC concerning ten minute hit confirmations as explained in the SLED/CJICS NCIC Operating Manual, pg. I-37, 4.3, (A) and any future SLED/CJICS-FBI/NCIC updates.

7.9 Handling Serious Error Messages.

This agency adopts as its policy the procedures set forth by SLED/CJICS-FBI/NCIC concerning serious error messages as explained in the SLED/CJICS NCIC Operating Manual, pgs. I-25 through I-27, 3.2.2 and 3.2.3.

7.10 Validation of Records.

This agency adopts as its policy the procedures set forth by SLED/CJICS-FBI/NCIC concerning validation checks and quality control as explained in the SLED/CJICS NCIC Operating Manual, Part 11.

It is understood that the anniversary validation (once every year) that is required by FBI/NCIC for every record on file gives our agency only a bare minimum of protection. Therefore, it is also our policy to effectively review and validate all of the records in NCIC on a monthly basis. A control list (automated if possible) of all persons and items entered into NCIC by our department will be used in reviewing cases that may have had arrests of offenders, locates/returns of missing persons and recoveries of property.

7.11 Wanted Person File.

This agency adopts as its policy the procedures set forth by FBI/NCIC concerning wanted person records as explained in the SLED/CJICS NCIC Operating Manual, Part 7.

SLED/CJICS-FBI/NCIC Policy states that "Agencies that enter records in NCIC are responsible for their accuracy, timeliness and completeness" (pg. I-24, 3.1.1).

"NCIC records must be entered promptly to ensure maximum system effectiveness" (pg. I-24, 3.1.3). "Complete, accurate and timely records are essential to ensure system integrity. Users also are encouraged to enter records in a timely manner to afford the maximum protection to the law enforcement officer by providing up-to-date information. ...delayed entry of records in NCIC reduces or eliminates the possibility of apprehending wanted persons, locating missing persons and recovering stolen property" (SLED/CJICS NCIC Operating Manual, pg. I-7, 1.7).

Wanted person records will be entered by this agency as soon as proper documentation (i.e. the arrest warrant, incident report) has been completed. Enforcement supervisors will insure that wanted person reports are given to terminal operations as soon as possible.

Wanted person records will be removed from NCIC immediately upon receiving written confirmation that the wanted person has been apprehended.

Enforcement supervisors (uniformed patrol, detectives, warrant division, etc.) will insure that appropriate documentation is completed and forwarded to the terminal operators whenever warrants are served on persons who have records in the wanted person file.

NOTE OF CAUTION: Failure to insure that timely, accurate and complete information is entered in NCIC could endanger police officers and the public and could place both the entering agency and the locating agency in an awkward and possibly civilly liable position.

7.12 Missing Person File.

This agency adopts as its policy the procedures set forth by FBI/NCIC concerning missing person records as explained in the SLED/CJICS NCIC Operating Manual, Part 8.

SLED/CJICS-FBI/NCIC Policy states that "Agencies that enter records in NCIC are responsible for their accuracy, timeliness and completeness" (pg. I-24, 3.1.1). "NCIC records must be entered promptly to ensure maximum system effectiveness" (pg. I-24, 3.1.3). "Complete, accurate and timely records are essential to ensure system integrity. Users also are encouraged to enter records in a timely manner to afford the maximum protection to the law enforcement officer by providing up-to-date information. ...delayed entry of records in NCIC reduces or eliminates the possibility of apprehending wanted persons, locating missing persons and recovering stolen property" (SLED/CJICS NCIC Operating Manual, pg. I-7, 1.7).

NOTE OF CAUTION: Failure to ensure that timely, accurate and complete information is entered in NCIC could place both the entering agency and the locating agency in an awkward and possibly civilly liable position.

Missing person records will be entered by this agency as soon as proper documentation (i.e. the incident report) has been completed. Prompt entry of the missing person record in NCIC will increase the likelihood of locating the missing person. Enforcement supervisors will insure that missing person reports are given to terminal operations as soon as possible.

Officers will make every effort to obtain dental and other descriptive information.

Enforcement supervisors (uniformed patrol, detectives, warrant division, etc.) will insure that appropriate documentation is completed and forwarded to the terminal operators whenever missing persons are located.

The case officer will be responsible for calling back or following up on missing persons within seventy-two (72) hours to determine any change of status of the case.

All officers/investigators involved with missing person cases will be familiar with and use the FBI/NCIC "Missing Person File-Data Collection Entry Guide" Packet. Completing the requested information in the packet insures proper entry of the missing person(s) in NCIC. FBI/NCIC policy states that agencies that enter records in NCIC are responsible for their completeness (pg. I-2, 1.3).

NOTE: Copies of the "Data Collection Entry Guide" packet may be obtained by contacting the Missing Person Information Center (MPIC) at SLED Headquarters (803/737-9000).

7.13 Stolen Vehicle File.

This agency adopts as its policy the procedures set forth by FBI/NCIC concerning stolen vehicle records as explained in the SLED/CJICS NCIC Operating Manual, Part 1.

SLED/CJICS-FBI/NCIC Policy states that "Agencies that enter records in NCIC are responsible for their accuracy, timeliness and completeness" (pg. I-24, 3.1.1). "NCIC records must be entered promptly to ensure maximum system effectiveness" (pg. I-24, 3.1.3). "Complete, accurate and timely records are essential to ensure system integrity. Users also are encouraged to enter records in a timely manner to afford the maximum protection to the law enforcement officer by providing up-to-date information. ...delayed entry of records in NCIC reduces or eliminates the possibility of apprehending wanted persons, locating missing persons and recovering stolen property" (SLED/CJICS NCIC Operating Manual, pg. I-7, 1.7).

Failure to ensure that timely, accurate and complete information is entered in NCIC could place both the entering agency and the locating agency in an awkward and possibly civilly liable position.

Stolen vehicle records will be entered by this agency as soon as proper documentation (i.e. the incident report) has been completed. Enforcement supervisors will insure that stolen vehicle reports are given to terminal operations as soon as possible.

NOTE OF CAUTION: Failure to immediately enter a stolen vehicle into NCIC could prevent the possibility of quickly locating the vehicle (and possible subjects) before time and distance become a significant factor in the case. A vehicle that is not entered in NCIC will not be reflected in an inquiry run by another agency that has that vehicle stopped. To repeat, should a vehicle not be entered in NCIC by the originating agency and should that vehicle be stopped by another police agency, the inquiry and reply from NCIC would not reflect that the vehicle was stolen. This could place the officers stopping the vehicle in great danger (not knowing the vehicle is stolen) and would focus great liability on the originating agency for not entering the vehicle in a timely manner.

Enforcement supervisors (uniformed patrol, detectives, warrant division, etc.) will insure that appropriate documentation is completed and forwarded to the terminal operators whenever stolen vehicles are recovered.

7.14 Other NCIC Files (Articles, License Plates, Boats, Guns, etc).

Along with the wanted person file, the missing person file and the stolen vehicle file, this agency adopts as is policy the procedures set forth by FBI/NCIC concerning Articles, License Plates, Boats, Guns, Securities etc. as explained in the current SLED/CJICS NCIC Operating Manual.

Records referred to in this section will be entered by this agency as soon as proper documentation (i.e. the incident report) has been completed. Enforcement supervisors will insure that these reports are given to terminal operations as soon as possible.

7.16 Routine Inquiry in NCIC.

It is the policy of this department to inquire in NCIC on all persons (offenders) taken into custody. This will be the responsibility of the booking officer. Furthermore, it is also the policy of this department to inquire in NCIC on all arrestees before being released from jail.

This procedure insures that wanted persons are identified and not released into the public.

Enforcement supervisors (uniformed patrol, detectives, warrant unit, etc.) will insure that appropriate documentation is completed and forwarded to the terminal operators so that they will conduct the inquiry.

NOTE OF CAUTION: Failure to inquire in NCIC (before release) on a subject in custody could cause a wanted person to be released who could possibly cause unnecessary harm or injury to police officers and the public. In such a case, great liability could be focused on this agency for failing to determine the status of the arrestee.

7.17 Disposing of Sensitive Information.

It is the policy of this agency to dispose of information (criminal history, etc.) that is not to be kept or filed, by either burning or shredding. To quote from the SLED/CJICS NCIC Operating Manual, pg. 10-10, (C), (3): "copies of criminal history data obtained from terminal devices must be afforded security to prevent any unauthorized access to or use of that data."

It shall be the duty and responsibility of all supervisors in this agency to make certain that the proper procedures for the destruction of criminal history data are followed.

The destruction of such data will be by burning or shredding as soon as it is determined the information is no longer needed or necessary.



City of Myrtle Beach
Police Department

SOUTH CAROLINA

MEMORANDUM

TO: ALL PATROL AND DETENTION PERSONNEL

**FROM: NCIC INSTRUCTOR AND TERMINAL AGENCY
COORDINATOR; RHONDA NOBLES**

DATE: JAN. 14, 2003

RE: LAPTOPS SECURITY

1. Laptops must be closed when transporting any inmate or victim to or from the station.
2. Laptops must be closed and vehicle must be locked when officer is out on a call, or just out of his/her vehicle, for any reason.
3. All officers must adhere to 1 & 2, not doing so will be a violation of NCIC Security policy.

VIOLATION OF SLED/CJICS-FBI/NCIC SYSTEM POLICIES

<u>Violation</u>	<u>1st Offense</u>	<u>2nd Offense</u>	<u>3rd Offense</u>
Unauthorized disclosure of receipt of Sled/CJICS- FBI/NCIC criminal justice info. * Group III (b)	Up to 5 days suspension to dismissal	Dismissal	N/A
Release of Drivers License or Vehicle reg. Information to other than Criminal Justice employee. * Group III (b)	Up to 5 days Suspension to Dismissal	Dismissal	N/A
Release of information to private security guards or firefighters * Group III (b)	Up to 5 days suspension to dismissal	Dismissal	N/A
Allowing the use of the system by personnel not certified by SLED, except for job training towards certification *Group III (a), (b), or (k)	Up to 5 days suspension to dismissal	Dismissal	N/A
Failure to comply with policies and procedures established in the MBPD and Sled/CJICS Procedures Manual *Group I (f) or Group III (A) or Group III (K)	Oral reprimand to Dismissal	Written reprimand to dismissal	Up to 5 days suspension or dismissal
Failure to log information supplied to the Coroner's office, the Solicitor's office, or any other Criminal Justice employee who does not have a user agreement with MBPD *Group I (f)	Oral reprimand	Written reprimand	Up to 5 days suspension or dismissal
Improper Record Keeping Group I (f)	Oral reprimand	Written reprimand	Up to 5 days suspension or dismissal
* Referral to City Policy			

VALIDATION PROCEDURES FOR THE MYRTLE BEACH POLICE
DEPARTMENT, MYRTLE BEACH SOUTH CAROLINA

Upon receiving the Validation Letter from SLED/CJICS the CTA OR ASSISTANT CTA will go to the index card files and pull the corresponding card and, run the item, wanted or missing person and or vehicle/motorcycle to ensure that the entry still exist and then make the proper notification to the owner of said item, and or vehicle/motorcycle either via phone call to the subject or via mail notification. Upon verification of the property the CTA or Assistant CTA will either validate or remove property from NCIC. Once the property in question is removed if that is the case the CTA or Assistant CTA will then run the property again to ensure that it is in fact removed from the SLED/CJICS computer system.

If the entry is in the wanted/missing person phase then the same notification must be make and the CTA or Assistant CTA must make sure that they are speaking to the reporting person, only the reporting person can verify whether or not the missing person has or has not been located. The CTA or Assistant CTA must contact the Clerk of Court to ensure that on a wanted person the warrant still exist and that the warrant has not been withdrawn. If the warrant has been withdrawn then that wanted person must be canceled from NCIC.

Validations are now to be performed on-line only. Records will be automatically purged if they are not validated, within the time frame.

The CTA or Assistant CTA will ensure that the Validation procedures are followed that all supporting documents are on file for the entries that are to remain in NCIC.

ANY QUESTIONS CAN BE DIRECTED TO CTA-Rhonda Nobles or Assistant CTA'S Nancy Medlin or Jean Smith.



MYRTLE BEACH POLICE DEPARTMENT

ADMINISTRATIVE REGULATIONS AND OPERATING PROCEDURES

Subject: *Departmental Computer Resources*

Number: *109-A*

Effective Date: *January 1, 2001*

Revised Date: *9-22-03*

Rescinds: *049*

Dated: *March 9, 2000*

Approved By:

PURPOSE

To establish procedures for the use of computer resources within the Department and to outline parameters for use of software, hardware and data to protect the interests of the Department and its employees.

DEFINITIONS

1. Computer System - All internal and external hardware components of the Departmental computer resources (PC stand alone, PC network, AS/400 mainframe, laptops, cabling, hubs, printers, servers, etc.)
2. Software - Programs used by a computer to perform any of its functions (i.e., DOS, MS Office Word, Excel, Access, Publisher etc.).
3. Authorized Software - Computer programs that the Department or city has paid for or is otherwise licensed. Also, personally owned or public domain software approved by the Chief of Police or his/her designee for use on a Departmental computer.
4. Data File - Word processing, spreadsheet, database or other file containing information, as opposed to software, which acts on a data file.
5. Computer System Administrator (SA) - A Departmental employee designated by the Chief of Police to work with the designated Public Safety MIS employee to (among other things) maintain all departmental computer equipment and ensure functional operating systems as well as guaranteeing proper job related application of the related hardware and software.

6. Computer Work Request Form – A form designed by the Systems Administrator that will be used by all department personnel to request assistance, or to have assistance authorized, when addressing computer needs that are of a moderate or highly technical nature.

PROCEDURE

1. This Department will maintain and use all available computer resources in accordance with all applicable Federal, State and Local laws, software manufacturer licensing agreements and departmental rules and regulations.

- A. At no time shall any software be installed or used on any departmental computer system in violation of copyright laws or this policy.
- B. According to the U.S. Copyright law, illegal reproduction of software or use of illegally copied software is subject to civil damages of \$50,000.00 or more in addition to criminal penalties that can include fines and/or imprisonment.
- C. Any employee who knowingly makes, acquires or uses unauthorized copies of computer software licensed to the Department or who places or uses unauthorized software on Departmental computer equipment shall be subject to immediate disciplinary action up to and including termination.
- D. The Myrtle Beach Police Department cannot condone and specifically forbids the unauthorized duplication of software.
- E. The intentional corruption of any information stored in the City computers or the unauthorized documentation of information shall result in disciplinary action.
- F. At no time will any employee sign on or allow someone to sign onto ANY computer using any log on name & password other than their own unless authorized by the Systems Administrator for maintenance or auditing purposes. The only exception to this will be when an employee's supervisor uses the employee's name and password to sign on to their workstation computer for authorized departmental business.

PROCEDURE

1. THE SYSTEMS ADMINISTRATOR will be appointed by the Chief of Police and will work under the Support Services Division with the Public Safety MIS employee. The Systems Administrator will be responsible for the following:

- A. Establish guidelines for the procurement of computer hardware, software, and supplies; maintenance of computer hardware/software; use of computer hardware/software; and inventory of all computer resources.
- B. Review requests from employees for computer systems hardware/software and make appropriate recommendations.
- C. Evaluate and make decisions to approve or disapprove requests for use of personally owned computer hardware/software.
- D. Coordinate the acquisition of all Departmental computer hardware/software products with the Public Safety MIS.
- E. Coordinate the installation, use, inspection, and support of Departmental computer systems with the Public Safety MIS. Conduct random inspections of computer resources used by Departmental employees.
- F. Coordinate requests for computer training, information and assistance.
- G. Identify qualified personnel in each division who will be authorized by the Systems Administrator to assist him/her in the performance of the above listed duties.

2. ALL DEPARTMENT SUPERVISORS

- A. Ensure that all Department members comply with all applicable statutes, software manufacturers' licensing agreements and Departmental rules and regulations concerning the use of all computer resources used by employees.
- B. Direct any requests for computer assistance to the Systems Administrator via a Computer Work Request Form. If the Systems Administrator has identified assisting personnel in the division where the request for assistance originates, the supervisor may instead consult with that person. At the time of his/her appointment, the Systems Administrator will have discussed with the assisting person exactly what activities he/she may perform at his/her level without first seeking Systems Administrator assistance. This type of work will be limited to routine day-to-day issues and minor repair, diagnostics, configurations and upgrades. For this type of work to be completed, it is not necessary that a Computer Work Request Form be filled out. The assisting person will routinely communicate with the Systems Administrator and/or MIS employee concerning their activities in their respective division. They will also immediately report any recurring lower level maintenance issues that they identify so that the Systems Administrator and/or MIS employee may evaluate it with respect to the overall operating system. Any computer

related work that is determined by the Systems Administrator to be moderately technical or very technical in nature would require that a Computer Work Request Form be filled out prior to the assistance being offered. The Systems Administrator, the MIS employee or their designated and qualified representative will complete the work.

- C. Report any damaged or vandalized computer equipment to the Systems Administrator via a Computer Work Request Form.
- D. All damage must be logged on a Loss Report and forwarded through the chain of command with a copy forwarded to the Systems Administrator. The form should include, but is not limited to, the damage incurred, the serial number, model, brand name, city ID number, and location of the equipment.

3. COMPUTER USERS

- A. Must comply with all State and Local Laws, software manufacturers' licensing agreements and Departmental rules and regulations.
- B. Provide the Systems Administrator, identified assisting division personnel, and immediate supervisor with any changed passwords to the assigned computer or logins.
- C. Make periodic backup copies of all critical or sensitive data files and maintain these in a secure location.
- D. Notify their supervisor, Systems Administrator, and identified assisting division personnel in the event of a system hardware or software problem for appropriate resolution.

4. UTILIZATION OF COMPUTER RESOURCES

- A. All computer equipment is provided for Departmental business and other uses that are approved by the City's Computer Use Policy. Any use for personal or financial gain, outside of these specific guidelines, is prohibited and may result in disciplinary action.
- B. All information stored within Departmental computer systems shall be considered official business and therefore is the property of the Myrtle Beach Police Department. All information within the computers is subject to inspection and will be audited randomly.
- C. All data created or stored on Departmental computer systems will be used solely for law enforcement purposes and other activities that are expressly authorized by City policy.

- D. Employees will make every reasonable attempt to ensure that no software that is to be used in a departmental computer is contaminated with a virus. At any time that an employee does identify or suspect a virus has infected his/her workstation, he/she will immediately shut down the computer and promptly notify the System Administrator, identified division assisting personnel or other City of Myrtle Beach IS employee.

5. TRANSFER OR SEPARATION FROM EMPLOYMENT

- A. When an employee, for any reason, separates from employment with the Department, the employee will surrender all data files produced and/or maintained by said employee.
- B. Any employee who transfers within the Department will release any and all data, files, etc within their possession relating to the previous position to the employee's immediate supervisor.

6. TRANSFER OF COMPUTER EQUIPMENT

- A. All transfer of computer equipment must be coordinated through the Systems Administrator.

7. ONLINE SERVICES

- A. Employees may not access any online service with a Departmental computer or under a Departmental address, or incur online service charges, without proper specific or implied authorization from the Chief of Police or the Systems Administrator. All online activity will comply with guidelines outlined throughout this policy and the City's Computer Use Policy.
- B. Employees may not access nor download any data, graphics, photos, websites, etc., from any internet or intranet website with any departmental computer or any computer under the direct control of the department unless required for investigative, intelligence or work related research. Downloads of material designed to improve the function of the assigned computer, or its components, with the approval of the System Administrator or identified assisting division personnel will be authorized.



City of Myrtle Beach
MIS Request Form

First in Service

Date: _____

Department: _____

Name: _____

Phone Ext: _____

Priority: ☐ Routine ☐ Preventive Maintenance ☐ Emergency

Description of work needed: _____

Signature of Requesting Employee: _____

FOR MIS USE ONLY

Assigned to: _____ Date: _____

Completed: ☐ Date Completed: _____

Comments: _____

Request Number:

SOUTH CAROLINA LAW ENFORCEMENT DIVISION

MARK SANFORD
Governor

ROBERT M. STEWART
Chief



TECHNICAL SECURITY AUDIT SEGMENT

This Questionnaire is being sent to your agency approximately one month prior to your routine NCIC on-site audit. Please answer all of the questions and please return this segment to me as soon as possible so our Information Security Officer will have time to review it before the audit. For the very technical questions (i.e. Encryption, Internet Access, Firewalls, etc.) you may want to receive assistance from your technical support staff/person. Attaching a diagram or diagrams to this questionnaire to explain certain technical issues may be helpful. Your local agency security officer must complete sections 5 and 6.

Any questions, please contact Sharon Baron at 803-896-7109.

When completed, please return this Questionnaire along with any pertinent information to:

Robin Gilmore, Mail-In Auditor
S. C. Law Enforcement Division
Post Office Box 21398
Columbia, S.C. 29221-1398

Some Responsibilities of the Local Agency Security Officers

- Serve as the security point of contact (POC) for the state or federal ISO (Information Security Officer) at the local agency;
- Know who is using the equipment and how the equipment is connected to the CJIS systems;
- Ensure that no untrained personnel are using CJIS system terminals;
- Ensure that hardware has the appropriate security measures in place;
- Keep the ISO informed of security incidents;
- Support policy compliance at the local agency in partnership with the ISO;
- Work closely with the agency's TAC & ATAC.



An Accredited Law Enforcement Agency

P.O. Box 21398/ Columbia, South Carolina 29221-1398/ (803) 737-9000/ Fax (803) 896-7041

TECHNICAL SECURITY AUDIT SEGMENT

Have your IT Person answer all of the questions and then return this segment along with your Mail-In Audit Questionnaire. Attaching a diagram or diagrams to this questionnaire to explain certain technical issues may be helpful. **Your local agency security officer must complete sections 5 and 6. If you have any questions, please contact Sharon Baron at 803-896-7109.**

When completed, please return this Questionnaire along with any pertinent information to:

Attn: Robin Gilmore, Mail-In Auditor
S.C. Law Enforcement Division
Post Office Box 21398
Columbia, S.C. 29221-1398

Who is your agency's appointed Local Agency Security Officer (LASO)?

(Name & title/rank)

(Phone number)

(Name of the organization or company of the local agency security officer)

Is the LASO aware of his/her LASO duties & responsibilities as defined by the FBI Security Policy?

☐ Yes ☐ No

Does your agency receive **South Carolina Law Enforcement Division CJIS** and National Crime Information Center (NCIC) service through an interface or a central communications/ regional dispatch center (RDC)?

☐ Yes ☐ No

If yes, is the interface/RDC owned, managed, and operated by a criminal justice agency?

☐ Yes ☐ No

If no, who owns, operates, and manages the interface and/or RDC?

- _____

☐ Non Criminal Justice Agency
☐ Private Contractor
☐ Non Governmental Agency
☐ Other

Please enclose copy of agreement(s)/maintenance contract(s) between your agency and software & hardware vender(s).

Has your agency developed and adopted a written Technical Security Policy?

☐ Yes ☐ No

IMPORTANT: An agency's Technical Security Policy should include requirements (for Physical Security, Internet Access, etc.) mentioned in the FBI CJIS Security Policy and in the SLED CJIS Technical Security Policies.

I. PERSONNEL BACKGROUND SCREENING

What type of Background Screening is required for Terminal operators?

- ☐ Fingerprinting
- ☐ III
- ☐ State Criminal History
- ☐ DMV Files

State and National fingerprint-based record checks must be conducted within 30 days upon initial employment for all personnel, including appropriate IT personnel, having access to FBI CJIS systems information. Does agency comply?

☐ Yes ☐ No

Agencies must also screen custodial, support and/or contractor personnel accessing the terminal areas through established personnel background screening methods, unless escorted by authorized personnel. Does agency comply?

☐ Yes ☐ No

Is the agency aware of the FBI CJIS Policy "If a felony conviction of any kind is found, access will not be granted"?

☐ Yes ☐ No

According to current SLED NCIC Personnel Security Procedures, "No person will be allowed access to NCIC or the state CJIS network in any case where a record check reveals:

1. A pending indictment;
2. A felony conviction;
3. A misdemeanor conviction for crimes of violence, sexual assault, molestation, exploitation or prostitution or
4. Any other misdemeanor conviction if such conviction bears on an individual's fitness for access to sensitive law enforcement information."

Is your agency aware of this policy?

☐ Yes ☐ No

Does your agency comply with this policy?

☐ Yes ☐ No

II. STANDARDS FOR DISCIPLINE

Written Standards for Discipline is an FBI requirement for agencies having access to FBI CJIS information. Agencies must have this disciplinary policy as part of their adopted, written SOP. This disciplinary policy must be in place for the agency to handle FBI NCIC SLED CJIS policy violators. The agencies technical security policy should address the following areas:

- | | |
|---|--|
| Unauthorized modification or destruction of system data | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Loss of computer system processing capability | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Loss by theft of any computer system media including | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Chip ROM memory | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Optical or magnetic storage medium | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| Hardcopy printout, etc. | <input type="checkbox"/> Yes <input type="checkbox"/> No |

III. PHYSICAL SECURITY

The computer site must be secure (protected from unauthorized use and viewing) as well as locations or vehicles housing MDTs or laptop computers capable of accessing FBI CJIS record information.

Does your agency comply?
☐ Yes ☐ No

All visitors to the computer centers and/or terminal areas must be accompanied by authorized personnel at all times.

Does your agency comply?
☐ Yes ☐ No

FACSIMILE TRANSMISSION PROCEDURES

A facsimile device may be used to transmit hardcopy criminal history records provided both agencies involved have an NCIC ORI authorized to receive criminal history information. Telephone notification prior to the transmission of information should be initiated to verify the authenticity of the receiving agency.

Does your agency comply?
☐ Yes ☐ No ☐ NA

MOBILE DATA TERMINALS

Does your agency have Mobile Data Terminals (MDTs)?

☐ Yes ☐ No

If Yes, How many MDTs does your agency have? _____

Each individual authorized for access shall be uniquely identified (full name, badge #, serial number or other unique alphanumeric identifier).

☐ Yes - Type of ID: _____

☐ No

How are passwords kept safe by the agency?

Are passwords changed?

☐ Yes ☐ No

If yes, how often?

Who changes the passwords?

Are passwords changed when employees (with access) are terminated?

☐ Yes ☐ No

Is programming in place to conduct proper authentication for use of the system?

☐ Yes ☐ No

Can the MDTs be used to:

Make hot file inquiries?

☐ Yes ☐ No

Make hot file entries?

☐ Yes ☐ No

Access III information?

☐ Yes ☐ No

Access state criminal history information?

☐ Yes ☐ No

Access state motor vehicle registration files?

☐ Yes ☐ No

What level of certification training do MDT operators have?

Are all MDT operators certified?

☐ Yes ☐ No

If No, explain:

Describe the Physical Security Requirements for securing MDTs from unauthorized access (i.e., locked doors, not in use when prisoner in car, etc):

Does your agency have an MDT Security Policy?

☐ Yes ☐ No

Please attach a copy of your MDT Security Policy.

LAPTOP COMPUTERS (if access to FBI CJIS information)

Does your agency have laptop computers accessing FBI CJIS information?

☐ Yes ☐ No

Each individual authorized for access shall be uniquely identified (full name, badge #, serial number or other unique alphanumeric identifier.

☐ Yes - Type of ID: _____

☐ No

How are passwords kept safe by the agency?

Are passwords changed?

☐ Yes ☐ No

If yes, how often?

Who changes the passwords?

Are passwords changed when employees (with access) are terminated?

☐ Yes ☐ No

Is programming in place to conduct proper authentication for use of the system?

☐ Yes ☐ No

Does your agency have laptop computers accessing FBI CJIS information?

☐ Yes ☐ No

If Yes, can the laptop computers be used to:

Make hot file inquiries? Make hot file entries?

☐ Yes ☐ No

Access III information?

☐ Yes ☐ No

Access state criminal history information?

☐ Yes ☐ No

Access state motor vehicle Registration files?

☐ Yes ☐ No

Describe the Physical Security Requirements for securing laptop computers from unauthorized access:

Please attach a copy of your laptop computer Security Policy.

[NOTE: A strong suggestion from the FBI: Make sure ALL personal computers in your agency are equally protected-hackers look for the "weakest" terminal.]

Are ALL of the agency's PCs equally protected?

☐ Yes ☐ No

IV. ADMINISTRATIVE SECURITY

Each local agency having access to a criminal justice network shall have someone designated as the Security Point-of-Contact (POC).

Name your POC:

User Agreements (User Agreement & System Responsibilities, Serviced Agency Addendum, Non-terminal and MDT (if applicable)) must be current and in place.

☐ Yes ☐ No

Does your agency routinely conduct a security assessment to include an analysis of threats, vulnerabilities, risks, architecture, protocols, operational, physical and employee security, etc?

☐ Yes ☐ No

(A good security policy should consider both outside and inside threats & intrusions)

Are non-criminal justice governmental agencies authorized to receive FBI CJIS systems information pursuant to Executive Order, statute, regulation or inter-agency agreement?

☐ Yes ☐ No ☐ NA

If a private contractor is involved, is a "Security Addendum" current, signed and in place?

☐ Yes ☐ No ☐ NA

V. TECHNICAL SECURITY

IDENTIFICATION:

Each individual authorized for access shall be uniquely identified (full name, badge #, serial number or other unique alphanumeric identifier).

☐ Yes – Type of ID: _____

☐ No

How are passwords kept safe by the agency?

Are passwords changed?

☐ Yes ☐ No

If yes, how often?

Who changes the passwords?

Are passwords changed when employees (with access) are terminated?

☐ Yes ☐ No

AUTHENTICATION:

Is programming in place to conduct proper authentication for use of the system?

☐ Yes ☐ No

As part of this review, you must attach a simplified network diagram, along with a brief narrative description of measures taken to ensure the security of the CTA System. Show placement of the following:

WIRELESS UPGRADES
ENCRYPTION
DIAL-UP ACCESS
INTERNET ACCESS
FIREWALLS

WIRELESS:

Upgrades contracted after 1-1-01 shall support a minimum of 128-bit encryption for all data. (Systems contracted prior to April 1999 do not require encryption at this time.)

Does your system comply with this policy?

☐ Yes ☐ No

ENCRYPTION:

All FBI CJIS information passing through a public network segment must be protected with encryption, while in that segment with it sanctionable as of September 30, 2002, except for good cause shown to the APB, not to be extended past 2005 (Sept. 30, 2005). Encryption shall employ at least a 128-bit key for systems contracted after I-I-OJ.

Does your system comply with this policy?

☐ Yes ☐ No

DIAL-UP ACCESS:

Each individual authorized for access shall be uniquely identified (full name, badge #, serial number or other unique alphanumeric identifier.

☐ Yes – Type of ID: _____

☐ No

How are passwords kept safe by the agency?

Are passwords changed?

☐ Yes ☐ No

If yes, how often?

Who changes the passwords?

Are passwords changed when employees (with access) are terminated?

☐ Yes ☐ No

Is programming in place to conduct proper authentication for use of the system?

☐ Yes ☐ No

The Interface Agency (SLED) has the authority to administer manage and monitor (during periodic audits) the security measures for Dial-up Access (to include user identity and agency association, the authorization of the user and level of access authorized, the purpose and frequency of use and the location of fixed-based dial-up sites).

All FBI CJIS transactions and messages sent and received on the Dial-up system must be logged. Conditions of maintaining the log must meet FBI CJIS Policy.

Does your system comply with this policy?

☐ Yes ☐ No

ACCESS CONTROL:

The implementation of Firewalls (to address network access control) must meet FBI CJIS Security Policy, 2000 and FBI CJIS Security Policy Implementation Guidelines.

Does your system comply with this policy?

☐ Yes ☐ No

INTERNET ACCESS:

Internet Access can be achieved only when a minimum set of technical and administrative requirements have been addressed and in place to assure the security of FBI CJIS systems from unauthorized access via the Internet. The technical requirements must address:

1. Advanced authentication, (e.g., digital signature and certificates, biometrics) to provide assurance that potential users are who they say they are;
2. Access control, (e.g., passwords and access control lists or smart cards and PINS) to prevent unauthorized access to a service or data;
3. Integrity, (e.g., configuration management and anti-virus software, digital signature and encryption) to detect unauthorized creation, alteration or deletion of data;
4. Confidentiality, (e.g., partitioned drives, encryption, and object reuse) to prevent the unauthorized disclosure of information and;
5. Non-repudiation (e.g., digital signatures and notarization) to prevent one partner in a transaction from denying that he/she has participated in all or part of the interaction.

Does your policy/system address these requirements?

☐ Yes ☐ No

LOGGING HOT FILES AND CRIMINAL HISTORY:

All agencies accessing NCIC hot files and III transactions must maintain an automated log on hot file transactions for a minimum of six months and III transactions for a minimum of twelve months. These logs must include unique operator identification, agency ORI requester and secondary recipient.

NCIC Policy requires that "all users must provide a reason for all III inquiries." This means that the Justification Field must be filled out to SLED CJIS guidelines.

Does your policy/system comply with this requirement?

☐ Yes ☐ No

"

SECURITY MONITORING:

Audit Trails must be developed to monitor and identify all illegal accesses and attempted illegal accesses that might have an impact on the FBI CJIS system.

Audit Trails should contain information required in the FBI CJIS Security Policy, 2000 (pg. 9).

Audit Trails should be reviewed at least once a week.

Security-related incidents that impact FBI CJIS data or communications circuits shall be reported by the agency's ISO in writing to the CSA (ISO) and FBI CJIS Division's ISO immediately.

Does your policy/system address these requirements?

☐ Yes ☐ No

VI. THE HANDLING OF SECURITY INCIDENTS AND VIOLATIONS

Does the agency have a written protocol on how to respond to system intrusions and the reporting of intrusions and violations?

☐ Yes ☐ No

This questionnaire was completed by: _____ (Print name)

_____ (Title)

_____ (Signature)

Date: _____

This questionnaire was completed by: _____ (Print name)

_____ (Title)

_____ (Signature)

Date: _____

This questionnaire was completed by: _____ (Print name)

_____ (Title)

_____ (Signature)

Date: _____